Deutscher Bundestag **Drucksache 16/7769**
16. Wahlperiode 16. 01. 2008

Beschlussempfehlung und Bericht

des Rechtsausschusses (6. Ausschuss)

zu der Unterrichtung durch die Bundesregierung
– Drucksache 16/7393 Nr. A 34 –

Vorschlag für einen Rahmenbeschluss des Rates zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung (inkl. 14960/07 ADD 1 und 14960/07 ADD 2) KOM(2007) 650 endg.; Ratsdok. 14960/07

A. Problem

Mit dem bestehenden Rahmenbeschluss 2002/475/JI zur Terrorismusbekämpfung werden innerhalb der EU Merkmale terroristischer Straftaten einheitlich bestimmt. Der Vorschlag der Europäischen Kommission zur Änderung des Rahmenbeschlusses soll – wie das Übereinkommen des Europarates zur Verhütung von Terrorismus vom 16. Mai 2005 – eine Verpflichtung der Mitgliedstaaten begründen, die öffentliche Aufforderung zur Begehung einer terroristischen Straftat sowie die Anwerbung und Ausbildung zu terroristischen Zwecken, insbesondere über das Internet, unter Strafe zu stellen. Darüber hinaus sollen die Mitgliedstaaten weitere Straftaten unter besonderen Umständen als terroristische Straftaten einstufen.

Im Rahmen eines Testlaufs, der auf Anregung der Konferenz der Ausschüsse für Gemeinschafts- und Europaangelegenheiten der Parlamente der Europäischen Union (COSAC) durchgeführt wird, ist vor der weiteren inhaltlichen Auseinandersetzung mit diesem Vorschlag zu prüfen, ob der Entwurf des Rahmenbeschlusses mit den Grundsätzen der Subsidiarität vereinbar ist. Hierzu soll innerhalb von acht Wochen Stellung genommen werden.

B. Lösung

Feststellung, dass keine Bedenken hinsichtlich der Einhaltung des gemeinschaftsrechtlichen Grundsatzes der Subsidiarität bestehen. Diese Feststellung wird im Falle der Annahme der Beschlussempfehlung als Stellungnahme des Deutschen Bundestages an die Präsidenten des Europäischen Parlaments, des Europäischen Rates und der Europäischen Kommission übermittelt.

Annahme einer Entschließung mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion DIE LINKE.

C. Alternativen

Keine

D. Kosten

Wurden im Ausschuss nicht erörtert.

Beschlussempfehlung

Der Bundestag wolle beschließen,

in Kenntnis der Unterrichtung durch die Bundesregierung auf Drucksache 16/7393 Nr. A 34 folgende Entschließung anzunehmen:

a) Der Bundestag stellt fest, dass der Vorschlag der EU-Kommission für einen Rahmenbeschluss des Rates zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung – KOM(2007) 650 endg.; Ratsdok. 14960/07 – keinen Bedenken hinsichtlich der Einhaltung des gemeinschaftsrechtlichen Grundsatzes der Subsidiarität begegnet.

b) Der Bundestag äußert Bedenken hinsichtlich der Einhaltung des gemeinschaftsrechtlichen Grundsatzes der Verhältnismäßigkeit durch den Vorschlag für einen Rahmenbeschluss.

c) Im Übrigen bleibt der Vorschlag für einen Rahmenbeschluss einer späteren Befassung vorbehalten.

Berlin, den 16. Januar 2008

Der Rechtsausschuss

Andreas Schmidt (Mülheim)
Vorsitzender

Siegfried Kauder (Villingen-Schwenningen)
Berichterstatter

Dr. Carl-Christian Dressel
Berichterstatter

Mechthild Dyckmans
Berichterstatterin

Wolfgang Neskovic
Berichterstatter

Jerzy Montag
Berichterstatter

Bericht der Abgeordneten Siegfried Kauder (Villingen-Schwenningen), Dr. Carl-Christian Dressel, Mechthild Dyckmans, Wolfgang Neskovic und Jerzy Montag

I. Überweisung

Das Ratsdokument 14960/07 wurde mit Überweisungsdrucksache 16/7393 (Nr. A 34) vom 3. Dezember 2007 gemäß § 93 Abs. 1 GO-BT dem Rechtsausschuss zur federführenden Beratung sowie dem Auswärtigen Ausschuss, dem Innenausschuss, dem Ausschuss für Menschenrechte und humanitäre Hilfe und dem Ausschuss für die Angelegenheiten der Europäischen Union zur Mitberatung überwiesen.

II. Stellungnahmen der mitberatenden Ausschüsse

Der **Auswärtige Ausschuss** hat die Vorlage in seiner 55. Sitzung am 16. Januar 2008 beraten und Kenntnisnahme empfohlen.

Der **Innenausschuss** hat die Vorlage in seiner 57. Sitzung am 16. Januar 2008 beraten und einvernehmlich festgestellt, dass der Subsidiaritätsgrundsatz gewahrt sei.

Der **Ausschuss für Menschenrechte und humanitäre Hilfe** hat die Vorlage in seiner 49. Sitzung am 16. Januar 2008 beraten und Kenntnisnahme empfohlen.

Der **Ausschuss für die Angelegenheiten der Europäischen Union** hat die Vorlage in seiner 48. Sitzung am 16. Januar 2008 beraten und mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP und BÜNDNIS 90/ DIE GRÜNEN gegen die Stimmen der Fraktion DIE LINKE. beschlossen, im Hinblick auf die Wahl der Rechtsgrundlage und das Subsidiaritätsprinzip keine Bedenken zu erheben.

III. Beratungsverlauf und Beratungsergebnis im federführenden Ausschuss

Der **Rechtsausschuss** hat die Vorlage in seiner 81. Sitzung am 12. Dezember 2007 erstmalig und in seiner 83. Sitzung am 16. Januar 2008 abschließend beraten. Er hat mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion DIE LINKE. beschlossen, dem Plenum zu empfehlen, keine Bedenken hinsichtlich der Einhaltung des Grundsatzes der Subsidiarität zu erheben, Bedenken hinsichtlich der Einhaltung der Verhältnismäßigkeit zu äußern und die weitere Befassung einem späteren Zeitpunkt vorzubehalten.

Die Beratung des Vorschlags für den Rahmenbeschluss erfolgte im Rahmen eines Testlaufs zur Subsidiaritätsprüfung, der auf einen Beschluss der COSAC hin durchgeführt wird. Der Deutsche Bundestag wurde gebeten, gemäß Artikel 6 des Protokolls Nr. 2 zum Vertrag von Lissabon über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit innerhalb einer Frist von acht Wochen eine Stellungnahme an die Präsidenten des Europäischen Parlaments, des Rates und der Kommission abzugeben, ob der vorgeschlagene Rahmenbeschluss mit dem Subsidiaritätsprinzip vereinbar ist. Die inhaltlichen Anforderungen an die Einhaltung des Subsidiaritätsprinzips ergeben sich aus Artikel 5 Abs. 2 des EG-Vertrags und Protokoll Nr. 30 zum Vertrag von Amsterdam über die Anwendung der Grundsätze der Subsidiarität und Verhältnismäßigkeit (im Folgenden: Protokoll). Der Rechtsausschuss kam zu dem Ergebnis, dass der Vorschlag den Anforderungen hinsichtlich der Subsidiarität entspricht. Allerdings hat er Bedenken bezüglich der Einhaltung des Grundsatzes der Verhältnismäßigkeit geäußert.

Der Rechtsausschuss kam mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN zu dem Ergebnis, dass der Vorschlag der Europäischen Kommission den Anforderungen des Subsidiaritätsprinzips entspricht. Ein Verstoß ist aus folgenden Erwägungen verneint worden:

Da die in dem Rahmenbeschluss geregelte Materie der konkurrierenden Zuständigkeit der Europäischen Gemeinschaft unterfalle, komme gemäß Artikel 2 EU-Vertrag in Verbindung mit Artikel 5 Abs. 2 EG-Vertrag (in der derzeit geltenden Fassung) das Subsidiaritätsprinzip zur Anwendung. Als Rechtsgrundlage könne Artikel 34 Abs. 2 Buchstabe b in Verbindung mit den Artikeln 29 und 31 Abs. 1 Buchstabe e EUV herangezogen werden, wonach die EU – wie im vorliegenden Rahmenbeschlussentwurf vorgesehen – zur Errichtung eines Raums der Freiheit, der Sicherheit und des Rechts Mindestvorschriften über die Tatbestandsmerkmale strafbarer Handlungen und die Strafen für terroristische Handlungen annehme. Für diese Materie besitze die EU nicht die ausschließliche Zuständigkeit.

Nach den in Nummer 5 des Protokolls enthaltenen Leitlinien entspreche der geplante Rahmenbeschluss den Anforderungen des Subsidiaritätsprinzips. Eine Regelung durch die Mitgliedstaaten könne das von der Europäischen Kommission verfolgte Ziel nicht ebenso gut erreichen.

Es handele sich um einen Rechtsbereich, für den transnationale Aspekte typisch seien. Außer von potentiell innerhalb eines Staates agierenden Terroristen gehe zunehmend von international agierenden Terrornetzwerken eine Gefahr aus. Insbesondere die gemäß dem geplanten Rahmenbeschluss zu bestrafende Verbreitung von terrorismusfördernden strafbaren Inhalten über das Internet habe in vielen Fällen grenzüberschreitenden Charakter.

Die Bekämpfung von Terrorismus und Cyberkriminalität auf EU-Ebene erforderte ein abgestimmtes Vorgehen der Mitgliedstaaten sowie eine Zusammenarbeit auf internationaler Ebene. Ein abgestimmtes Vorgehen werde durch die in dem Kommissionsvorschlag vorgesehene Vereinheitlichung strafrechtlicher Regelungen in den Mitgliedstaaten erleichtert. Zwar verfügten alle Mitgliedstaaten über strafrechtliche Bestimmungen in dem durch den Rahmenbeschluss zu regelnden Bereich, jedoch seien die Regelungen in Reichweite und Anwendungsbereich unterschiedlich. Für die von der Europäischen Kommission vorgeschlagenen Regelungen spreche insbesondere, dass dadurch die Strafverfolgung grenzüberschreitender terroristischer Aktivitäten erleichtert werde. Die in Artikel 9 des geltenden Rahmenbeschlusses

enthaltenen Vorschriften zur Gerichtsbarkeit und zur Strafverfolgung seien dann auch auf die von der Europäischen Kommission vorgeschlagenen neuen Tatbestände anwendbar. Außerdem würden die Kooperationsmechanismen der EU, wie sie zum Beispiel im Beschluss 2005/671/JI über den Informationsaustausch und die Zusammenarbeit betreffend terroristische Straftaten vorgesehen sind, ausgelöst werden, weil diese Mechanismen auf den Rahmenbeschluss anwendbar seien.

Des Weiteren lasse sich für die Notwendigkeit einer europäischen Regelung anführen, dass eine gemeinsame rechtliche Basis auch die Zusammenarbeit auf internationaler Ebene vereinfachen und dort die Position der EU stärken würde.

Die Mehrheit der Mitglieder des Ausschusses äußerte jedoch Bedenken hinsichtlich der Vereinbarkeit des Rahmenbeschlusses mit dem in Artikel 2 EU-Vertrag in Verbindung mit Artikel 5 Abs. 3 EG-Vertrag statuierten Grundsatz der Verhältnismäßigkeit. Da aber die Verhältnismäßigkeit im Rahmen des COSAC-Testlaufs nicht zu prüfen war, wurde diese Frage nicht abschließend behandelt.

Nach dem Grundsatz der Verhältnismäßigkeit dürften Maßnahmen der Europäischen Gemeinschaft bzw. Europäischen Union inhaltlich wie formal nicht über das zur Erreichung der Ziele der Verträge erforderliche Maß hinausgehen. Unter Zugrundelegung der in den Nummern 6 und 7 des Protokolls formulierten Leitlinien erscheine es allerdings fraglich, ob die von der Europäischen Kommission vorgeschlagenen Regelungen im Hinblick auf die Ziele des EU-Vertrags erforderlich seien. Eine Alternative zu dem vorgeschlagenen Rechtsakt könne darin bestehen, dass die Mitgliedstaaten sich in einer Entschließung dazu verpflichten, das Übereinkommen des Europarates zur Verhütung des Terrorismus vom 16. Mai 2005 bis zu einem bestimmten Zeitpunkt zu ratifizieren und umzusetzen. Die in den Artikeln 5 bis 8 dieses Übereinkommens enthaltenen Tatbestände seien deckungsgleich mit den von der Europäischen Kommission vorgeschlagenen Regelungen. Ein von allen EU-Mitgliedstaaten ratifiziertes Übereinkommen könne außerdem eine Vorbildwirkung über die Mitgliedstaaten hinaus entwickeln. Da eine Ratifizierung des Europaratsübereinkommens ohnehin von den Mitgliedstaaten abgestrebt werde, stelle sich die Frage, welchen rechtlichen und praktischen Mehrwert eine bloße Duplizierung von Vorschriften des Übereinkommens des Europarates in einem Rechtsakt der EU habe.

Die **Fraktion DIE LINKE.** äußerte Bedenken gegen die Mehrheitsauffassung.

Mit dem Vorschlag solle der Rahmenbeschluss des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (2002/475/JI, ABl. Nr. L 164 vom 22. Juni 2002 S. 3 bis 7) aktualisiert und durch die Aufnahme neuer Straftatbestände, wie die öffentliche Aufforderung zur Begehung einer terroristischen Straftat, Anwerbung für terroristische Zwecke und Ausbildung für terroristische Zwecke ergänzt werden. Der Vorschlag verfolge insoweit Zwecke, die sich teilweise mit dem Übereinkommen des Europarates vom 16. Mai 2005 (im Folgenden: ER-Übereinkommen) überschnitten, das die Vertragsparteien ebenfalls verpflichte, die öffentliche Aufforderung zur Begehung einer terroristischen Straftat, die Anwerbung und die Ausbildung für terroristische Zwecke unter Strafe zu stellen. Der Vorschlag enthalte einschließlich der Erwägungen zwölf Seiten in deutscher Sprache. Zur Begründung sei zugleich ein nur in englischer Sprachfassung vorgelegtes Arbeitsdokument vom 6. November 2007 (SEC (2007) 1424) beigefügt, das 106 Seiten umfasse.

Nach dem Subsidiaritätsprinzip werde die Gemeinschaft in den Bereichen, die nicht in ihre ausschließliche Zuständigkeit fallen, nur tätig, sofern und soweit die Ziele der in Betracht gezogenen Maßnahmen auf Ebene der Mitgliedstaaten nicht ausreichend erreicht werden könnten und daher wegen ihres Umfangs oder ihrer Wirkungen besser auf Gemeinschaftsebene ausgeführt werden könnten (Artikel 5 Abs. 2 EG-Vertrag). Das Prinzip werde im Protokoll Nr. 21 zum EG-Vertrag über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit (sog. Subsidiaritätsprotokoll) näher erläutert.

Zunächst sei die Wahl der Rechtsgrundlage zu untersuchen, da das Subsidiaritätsprinzip als Kompetenzausübungsregel nur zur Anwendung komme, wenn sich die Maßnahme auf eine nicht ausschließliche Gemeinschaftskompetenz stütze. Der Vorschlag sei auf die Artikel 29, 31 Abs. 1 Buchstabe e und Artikel 34 Abs. 2 Buchstabe b des EU-Vertrags gegründet. Danach seien Rahmenbeschlüsse zur Angleichung der Rechtsvorschriften, insbesondere Mindestvorschriften über die Tatbestandsmerkmale strafbarer Handlungen und die Strafen im Bereich des Terrorismus, zulässig. Es handele sich um eine nicht ausschließliche Kompetenz der Europäischen Union, auf die das Subsidiaritätsprinzip anzuwenden sei.

Im Übrigen setze das Subsidiaritätsprinzip voraus, dass die Ziele der in Betracht gezogenen Maßnahme durch die Mitgliedstaaten nicht ausreichend erreicht werden könnten. Nach den Leitlinien des Subsidiaritätsprotokolls sei dies der Fall, wenn der betreffende Bereich transnationale Aspekte aufweise, die durch Maßnahmen der Mitgliedstaaten nicht ausreichend geregelt werden könnten, oder wenn alleinige Maßnahmen der Mitgliedstaaten gegen Anforderungen des EG-Vertrags verstießen. Außerdem dürfe die Europäische Gemeinschaft nur tätig werden, wenn die Ziele der Maßnahmen wegen ihres Umfangs oder ihrer Wirkungen besser auf Gemeinschaftsebene erreichbar seien als auf mitgliedstaatlicher Ebene.

Ziel des Vorschlages und der Erwägungen, die zu seiner Vorlage geführt hätten, könnten vom mitgliedstaatlichen Gesetzgeber nur nachvollzogen und an den Erfordernissen der Subsidiarität gemessen werden, wenn sie umfassend und vollständig in der Amtssprache oder den Amtssprachen des Mitgliedstaates vorlägen. Eine sorgfältige Überprüfung der Einhaltung des Subsidiaritätsprinzips von Seiten des Deutschen Bundestages sei sonst nicht möglich. Das sei hier nicht der Fall. Auch aus diesem Grund könne nicht festgestellt werden, dass der Grundsatz der Subsidiarität gewahrt sei.

In ihrer Folgenabschätzung stelle die Europäische Kommission darauf ab, dass die modernen Informations- und Kommunikationstechnologien bei der Verbreitung des Terrorismus eine erhebliche Rolle spielten. Sie räume zwar ein, dass die überwiegende Zahl der Mitgliedstaaten über einschlägige Gesetze verfüge, verweise aber darauf, dass diese sich in ihrer Reichweite und ihrem Anwendungsbereich unterschieden. Die im Hinblick auf das Subsidiaritätsprinzip maßgebliche Fragestellung, welche tatsächlichen Lücken die Strafrechtsordnungen der Mitgliedstaaten enthielten, werde nur

oberflächlich behandelt. Zwar bestehe kein Zweifel daran, dass die Verbreitung von Informationen über das Internet grenzüberschreitenden Charakter haben könne. Die in der Begründung zum Entwurf des Rahmenbeschlusses unter der Überschrift „Subsidiarität“ aufgestellte Behauptung, Terroristen könnten sich die Unterschiede zwischen verschiedenen nationalen Rechtsordnungen und Gesetzeslücken zunutze machen, werde jedoch nicht überzeugend belegt.

Der Hinweis, dass die Aufnahme der neuen Straftatbestände in den Rahmenbeschluss 2002/475/JI die Anwendung der Koordinierungs- und Zusammenarbeitsmechanismen der polizeilichen und justiziellen Zusammenarbeit der Europäischen Union ermögliche, führe ins Leere. Durch die Einbeziehung bereits existierender Mechanismen werde notwendigerweise jede Zusammenarbeit soweit erleichtert, wie es das bestehende Instrument vorsehe. Somit könne das Ergebnis der Subsidiaritätsprüfung jederzeit durch die Bezugnahme auf bereits existierende Instrumente vorherbestimmt werden, so dass die Prüfung gegenstandslos sein würde.

Zudem sei es zwar richtig, dass auch eine materielle Rechtsvereinheitlichung die Koordination in verfahrensmäßiger Hinsicht erleichtern könne. Das reiche aber für die Notwendigkeit der vorgeschlagenen Änderungen nicht aus. Insofern müsse vielmehr überzeugend dargetan werden, dass eine Koordinierung bei Aufrechterhaltung unterschiedlicher materieller Regelungen so weit erschwert sei, dass ihre Funktionsfähigkeit infrage gestellt sei.

Die Tatsache, dass das ER-Übereinkommen praktisch gleich lautende Ziele verfolge, indem es die Unterzeichnerstaaten verpflichte, die öffentliche Aufforderung zur Begehung einer terroristischen Straftat, die Anwerbung und Ausbildung für terroristische Zwecke unter Strafe zu stellen, lasse den Änderungsvorschlag auch als Verstoß gegen den Grundsatz der Verhältnismäßigkeit erscheinen. Das ER-Übereinkommen sei zwar gegenwärtig (Stand 17. Dezember 2007) erst von sieben Staaten, darunter vier Mitgliedstaaten der EU (Bulgarien, Dänemark, Rumänien und die Slowakei), ratifiziert worden. Es könne aber nicht erwartet werden, dass Regierungen von Mitgliedstaaten, die bereit sind, dem Vorschlag zur Änderung des Rahmenbeschlusses zuzustimmen, das Ratifizierungsverfahren nicht ernsthaft betreiben würden.

Ingesamt sei zu beanstanden, dass der Vorschlag sowohl gegen die Zuständigkeitsordnung als auch gegen die Prinzipien der Subsidiarität und der Verhältnismäßigkeit verstoße.

Die Fraktion merkte ferner an, Ausgangspunkt der Subsidiaritätsprüfung sei die Frage, ob bei einer alleinigen Regelung auf europäischer Ebene erhebliche Beeinträchtigungen für die Mitgliedstaaten entstehen oder umgekehrt, ob die gemeinschaftsrechtliche Regelung deutliche Vorteile bringe. Dies sei nur zu subsumieren, wenn sämtliche Regelungen in den einzelnen Mitgliedstaaten bekannt seien. Die entsprechenden einzelstaatlichen Regelungen seien nicht zusammengetragen worden, so dass eine entsprechende Bewertung nicht möglich sei.

Die Vorlage des Referats Europa der Bundestagsverwaltung, die dem Mehrheitsvotum zugrunde liege, führe nur abstrakt aus, dass eine gemeinsame rechtliche Basis auch die Zusammenarbeit auf internationaler Ebene vereinfachen und dort die Position der EU verstärken werde. Die konkreten Subsumtionsschritte, die zu dieser Wertung hinführen, fehlten.

Die **Fraktion BÜNDNIS 90/DIE GRÜNEN** entgegnete, die Subsidiaritätsprüfung durch ein Parlament sei einer Subsumtion, die etwa ein Richter vornehme, nicht vergleichbar. Es handele sich vielmehr um eine rechtspolitische, summarische und bewertende Prüfung, die gegenüber einer Subsumtion im strengen Sinne stets kursorischen Charakter habe, weil anders auch kein zeitgerechtes Ergebnis zu erzielen sei. In diesem Rahmen habe eine intensive Auseinandersetzung stattgefunden, wie sich auch daran zeige, dass gegenüber der Vorlage des Referats Europa auf ihre Anregung an zwei Punkten Änderungen und Verbesserungen vorgenommen worden seien.

Die Fraktion äußerte trotz grundsätzlicher Zustimmung zur Mehrheitsauffassung einen Einwand in der Sache. Bei dem von der Mehrheit verwendeten Begriff „Cyberkriminalität“ handele es sich zwar um einen im Europarecht gebräuchlichen Begriff. Allerdings habe der Deutsche Bundestag die Bundesregierung aufgefordert, darauf zu dringen, dass dieser Begriff in der Zukunft konkretisiert werde, weil er nach deutschem Verständnis nicht bestimmt genug sei. Deshalb wäre es zur Verdeutlichung der Position des Rechtsausschusses und des Deutschen Bundestages besser gewesen, an dieser Stelle nur konkrete Fälle der Cyberkriminalität anzusprechen.

Die **Fraktion der SPD** erachtete den zweiten Testlauf zur Subsidiaritätsprüfung als sehr positive Erfahrung, die insbesondere zeige, dass es in dem vorgegebenen Zeitraum möglich sei, nicht nur bei der Subsidiaritäts- sondern auch – gleichsam überobligatorisch – in der Verhältnismäßigkeitsprüfung zu wohlbegründeten Ergebnissen zu kommen.

Zweifel bestünden jedoch, ob das Sekretariat des Rechtsausschusses mit der aktuellen Personalausstattung die Subsidiaritätsprüfung auch im künftig anstehenden Massenbetrieb werde unterstützen können. Dies müsse Gegenstand künftiger Haushaltsberatungen sein.

Problematisch würden auch in die parlamentarische Sommerpause fallende Subsidiaritätsprüfungen. Hier dürfe man sich nicht auf die Hoffnung verlassen, dass dieser Fall schon nicht eintreten werde. Vielmehr müsse die Handlungsfähigkeit des Rechtsausschusses sichergestellt werden. Hier bleibe abzuwarten, welche Erkenntnisse weitere Testläufe brächten.

An der Auffassung der Fraktion DIE LINKE. falle auf, dass die Tischvorlage in Wortlaut und Gliederung weitgehend der Stellungnahme des Ausschusses für die Angelegenheiten der Europäischen Union entspreche und nur zu anderen Wertungen gelange. Dies könne kaum als ausgiebige Auseinandersetzung mit der Mehrheitsmeinung angesehen werden.

Die **Fraktion der CDU/CSU** zeigte sich erfreut darüber, dass es dem Parlament in der Tat möglich sei, innerhalb der Frist von acht Wochen eine begründete Stellungnahme abzugeben. Dies sei indes nur dank der Hilfe des Ausschusssekretariats und des Bundesministeriums der Justiz möglich gewesen. Zu überlegen sei, wie künftig der durch diese Verfahren verursachte Mehraufwand zu bewältigen sei. Sollte das Ausschusssekretariat hierfür zuständig bleiben, werde die Erledigung dieser Aufgabe ohne Personalaufstockung nicht möglich sein.

In dem sehr ergiebigen Berichterstattergespräch hätten sich einige Verfahrensfragen ergeben, die in den nächsten Test-

läufen zu klären seien. Man sei eigentlich nur aufgefordert, zur Subsidiaritätsfrage Stellung zu nehmen. Offen sei auch geblieben, an wen die Stellungnahme des Rechtsausschusses weiterzuleiten sei.

Die **Fraktion der FDP** dankte dem Ausschusssekretariat und dem Referat Europa für die Unterstützung in diesem Testlauf. Im Regelbetrieb sei diese Aufgabe indes nicht ohne Personalzuwachs im Ausschusssekretariat zu leisten. Sie schließt sich den Ausführungen der Fraktion BÜNDNIS 90/DIE GRÜNEN zum Begriff „Cyberkriminalität“ an. Angesichts der häufig vorgebrachten Kritik des Deutschen Bundestages an diesem in den Listendelikten enthaltenen Begriff wäre es wünschenswert gewesen, konkrete Erscheinungsformen der Cyberkriminalität anzusprechen.

Die Äußerung zur Verhältnismäßigkeit sei sinnvoll, da im Hinblick auf das parallele Übereinkommen des Europarates große Bedenken hinsichtlich der Erforderlichkeit des Rahmenbeschlusses bestünden. Das Übereinkommen enthalte annähernd gleich lautende Straftatbestände und darüber hinaus immanente Schranken durch die Regelung von Bedingungen und Garantien im Hinblick auf Freiheitsrechte, die so in dem Rahmenbeschluss nicht vorgesehen seien. Hierzu zähle die Aufforderung an die Vertragsstaaten, das Recht auf freie Meinungsäußerung sowie die Vereinigungsfreiheit und die Religionsfreiheit sicherzustellen. Auch wenn die inhaltliche Prüfung noch bevorstehe, sei es sinnvoll, schon jetzt darauf hinzuweisen, dass der Rechtsausschuss keine Notwendigkeit für diesen Rahmenbeschluss sehe.

Berlin, den 16. Januar 2008

Der Rechtsausschuss

Siegfried Kauder (Villingen-Schwenningen)
Berichterstatter

Dr. Carl-Christian Dressel
Berichterstatter

Mechthild Dyckmans
Berichterstatterin

Wolfgang Neskovic
Berichterstatter

Jerzy Montag
Berichterstatter

Anlage

RAT DER EUROPÄISCHEN UNION

Brüssel, den 13. November 2007 (OR. en)

14960/07

Interinstitutionelles Dossier: 2007/0236 (CNS)

CATS 122
DROIPEN 104

VORSCHLAG

der:	Europäischen Kommission
vom:	12. November 2007
Betr.:	RAHMENBESCHLUSS DES RATES zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung

Die Delegationen erhalten in der Anlage den mit Schreiben von Herrn Jordi AYET PUIGARNAU, Direktor, an den Generalsekretär/Hohen Vertreter, Herrn Javier SOLANA, übermittelten Vorschlag der Kommission.

Anl.: KOM(2007) 650 endgültig

KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 6.11.2007
KOM(2007) 650 endgültig

2007/0236 (CNS)

Vorschlag für einen

RAHMENBESCHLUSS DES RATES

zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung

(von der Kommission vorgelegt)

{SEK(2007) 1424}
{SEK(2007) 1425}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

- **Gründe und Ziele des Vorschlags**

Der Terrorismus stellt eine der größten Gefahren für die Demokratie dar, bedroht die freie Ausübung der Menschenrechte und beeinträchtigt die Entwicklung von Wirtschaft und Gesellschaft.

Im Vertrag über die Europäische Union hat sich die EU das Ziel gesetzt, den Bürgern in einem Raum der Freiheit, der Sicherheit und des Rechts ein hohes Maß an Sicherheit zu bieten. Um dieses Ziel im Kampf gegen den Terrorismus zu erreichen, müssen die Mitgliedstaaten der Europäischen Union über wirksame Strafgesetze verfügen. Ebenso unerlässlich sind Maßnahmen zur Intensivierung der internationalen Zusammenarbeit in diesem Bereich.

Moderne Informations- und Kommunikationstechnologien spielen bei der Ausbreitung der terroristischen Bedrohung eine erhebliche Rolle. Dies gilt insbesondere für das Internet als preiswertes, schnelles und leicht zugängliches Medium mit praktisch globaler Reichweite. All diese Vorteile, die gesetzestreue Bürger, die das Internet tagtäglich nutzen, sehr zu schätzen wissen, machen sich auch Terroristen zunutze. Sie nutzen das Internet sowohl für die Verbreitung ihrer Propaganda, um Anhänger zu gewinnen und zu mobilisieren, als auch für die Verbreitung von Anleitungen und Online-Handbüchern für die Terrorismus-Ausbildung oder die Planung von Terroranschlägen. Adressaten sind Gefolgsleute ebenso wie Sympathisanten.

Das Internet trägt auf diese Weise maßgeblich zur Verstärkung des Radikalisierungs- und Rekrutierungsprozesses bei und dient darüber hinaus als „virtuelles Trainingscamp“, indem es Informationen über Mittel und Methoden des Terrorismus verbreitet. Die Verbreitung terroristischer Propaganda und Kenntnisse im Internet ergänzt und verstärkt die Indoktrinierung und Ausbildung in der realen Welt und trägt dazu bei, den Kreis terroristischer Aktivisten und Sympathisanten zu erweitern und zu festigen.

Dieser wachsenden Bedrohung Einhalt zu gebieten, ist eine politische Notwendigkeit. Die EU muss den modernen Terrorismus und seine neuen Vorgehensweisen mit der gleichen Entschlossenheit und Härte bekämpfen, die sie auch im Kampf gegen den Terrorismus herkömmlicher Art unter Beweis gestellt hat. Mit diesem Vorschlag soll der Rahmenbeschluss zur Terrorismusbekämpfung [ABl. L 164 vom 22.6.2002, S. 3-7] aktualisiert und durch Aufnahme neuer Straftatbestände wie öffentliche Aufforderung zur Begehung einer terroristischen Straftat, Anwerbung für terroristische Zwecke und Ausbildung für terroristische Zwecke dem Übereinkommen des Europarats zur Verhütung des Terrorismus angeglichen werden.

Diese Straftatbestände müssen vor allem aus folgenden Gründen in den Rahmenbeschluss zur Terrorismusbekämpfung aufgenommen werden:

– damit werden die Vorteile des stärker integrierten institutionellen Rahmens der Europäischen Union genutzt (insbesondere der Umstand, dass es keine langwierigen Unterzeichnungs- und Ratifizierungsverfahren wie bei Übereinkommen des Europarats gibt, dass besondere Follow-up-Verfahren vorgesehen sind, und dass eine für alle geltende Auslegung durch den Gerichtshof gewährleistet ist);

- der Rahmenbeschluss sieht spezifische Vorschriften in Bezug auf Art und Umfang der Strafen sowie zwingende Vorschriften betreffend die gerichtliche Zuständigkeit vor, die auch für die neu aufzunehmenden Straftatbestände gelten werden;
- der Rahmenbeschluss ist ein Schlüsselinstrument der EU-Strategie zur Terrorismusbekämpfung: die ausdrückliche Aufnahme dieser spezifischen vorbereitenden Handlungen lösen daher den Kooperationsmechanismus der EU mit Bezug zum Rahmenbeschluss aus.

Der zusätzliche Nutzen, der mit der Aufnahme der Straftatbestände der öffentlichen Aufforderung zur Begehung einer terroristischen Straftat sowie der Anwerbung und Ausbildung für terroristische Zwecke in die Terrorismus-Vorschriften der EU bewirkt wird, ist ausführlicher in der Folgenabschätzung beschrieben.

Der Rahmenbeschluss zur Terrorismusbekämpfung ist auch auf Verhaltensweisen anwendbar, die zu terroristischen Straftaten in Drittländern beitragen können. Damit bringt die Kommission ihre Entschlossenheit zum Ausdruck, sich weltweit und auf europäischer Ebene im Kampf gegen Terrorismus zu engagieren. Der vorliegende Änderungsvorschlag hält an diesem Konzept fest und unterstreicht die Bedeutung der internationalen Zusammenarbeit im Rahmen der bestehenden Einrichtungen und Kooperationsmechanismen.

Gleichzeitig ist dem Umstand Rechnung zu tragen, dass sich die Europäische Union und ihre Mitgliedstaaten der Achtung der Menschenrechte, der Grundfreiheiten und der Würde des Menschen sowie dem Schutz dieser Rechte gegenüber Einzelpersonen und Institutionen gleichermaßen verschrieben haben.

- **Allgemeiner Kontext**

Europäische Union

Der Rahmenbeschluss zur Terrorismusbekämpfung führt für alle Mitgliedstaaten eine einheitliche Definition terroristischer Straftaten ein und stellt sicher, dass für natürliche und juristische Personen, die solche Straftaten begangen haben oder dafür haften, Strafen und Sanktionen vorhanden sind, die der Schwere der Tat angemessen sind. Er legt fest, in welchen Fällen die Mitgliedstaaten verpflichtet sind, die gerichtliche Zuständigkeit für terroristische Straftaten zu übernehmen, damit diese wirksam verfolgt werden können. Aufgrund der Schutzbedürftigkeit der Opfer terroristischer Straftaten sind darüber hinaus besondere Schutz- und Unterstützungsmaßnahmen vorgesehen.

In ihrem ersten Bericht über die Durchführung des Rahmenbeschlusses zur Terrorismusbekämpfung [KOM(2004) 409 vom 8.6.2004 und Arbeitsdokument der Kommissionsdienststellen SEK(2004) 688 vom 8.6.2004] zog die Kommission Bilanz der auf nationaler Ebene getroffenen Durchführungsmaßnahmen. Der zweite Bericht, den die Kommission zeitgleich mit diesem Vorschlag angenommen hat, enthält eine Aktualisierung des Umsetzungsstands in den Mitgliedstaaten, die bereits im ersten Bericht behandelt wurden, sowie eine umfassende erste Bewertung des Umsetzungsstands in den Mitgliedstaaten, die im ersten Bericht noch nicht berücksichtigt waren. Beide Berichte geben Auskunft über den nach dem Erlass des Rahmenbeschlusses zur Terrorismusbekämpfung in der EU erreichten Harmonisierungsgrad und enthalten hilfreiche Auslegungsleitlinien sowie einen nützlichen Überblick über die einschlägige Gesetzgebung in den Mitgliedstaaten.

Wie der Europäische Rat im Haager Programm betonte, kann der Terrorismus bei uneingeschränkter Wahrung der Grundrechte nur wirksam verhütet und bekämpft werden, wenn sich die Mitgliedstaaten nicht nur auf ihre eigene Sicherheit konzentrieren, sondern die Sicherheit der Union insgesamt im Auge haben.

In der vom Rat „Justiz und Inneres“ im Dezember 2005 angenommenen EU-Strategie und dem Aktionsplan zum Thema Radikalisierung und Anwerbung werden Maßnahmen gefordert, um die Nutzung des Internets für terroristische Zwecke zu unterbinden. Gleichzeitig wird betont, dass Maßnahmen auf Ebene der Mitgliedstaaten mit Maßnahmen auf EU-Ebene einhergehen müssen.

In den Schlussfolgerungen des Europäischen Rats vom 15./16. Juni 2006 wurden Rat und Kommission ausdrücklich ersucht, unter Beachtung der Grundrechte und Rechtsgrundsätze Maßnahmen zur Bekämpfung des Missbrauchs des Internets zu terroristischen Zwecken auszuarbeiten.

Internationale Zusammenarbeit

Im Übereinkommen des Europarats zur Verhütung des Terrorismus (Warschau, 16. Mai 2005) werden die Vertragsparteien aufgefordert, dafür zu sorgen, dass die öffentliche Aufforderung zur Begehung terroristischer Straftaten sowie die Anwerbung und Ausbildung für terroristische Zwecke unter Strafe gestellt werden.

Relevant sind auf internationaler Ebene des Weiteren die Resolution 1624 des UN-Sicherheitsrats (14. September 2005) und die Weltweite Strategie der Vereinten Nationen zur Bekämpfung des Terrorismus (8. September 2006). Erwähnenswert sind auch der G8-Gipfel vom 16. Juli 2006 in St. Petersburg und der Beschluss des OSZE-Ministerrats Nr. 7/06 über die Bekämpfung der Nutzung des Internets zu terroristischen Zwecken.

- **Bestehende Rechtsvorschriften auf diesem Gebiet**

Nach Artikel 4 des Rahmenbeschlusses zur Terrorismusbekämpfung stellen die Mitgliedstaaten bei terroristischen Straftaten die Anstiftung, Mittäterschaft und den Versuch unter Strafe. Artikel 2 des Rahmenbeschlusses verpflichtet die Mitgliedstaaten, das Anführen einer terroristischen Vereinigung und die Beteiligung an den Handlungen einer solchen Vereinigung ebenfalls unter Strafe zu stellen. Diese Bestimmungen erstrecken sich jedoch nicht ausdrücklich auf die Verbreitung terroristischer Propaganda und Fachkenntnisse, insbesondere über das Internet.

Nach Artikel 5 bis 7 des Übereinkommens des Europarats zur Verhütung des Terrorismus werden die Vertragsparteien aufgefordert sicherzustellen, dass die öffentliche Aufforderung zur Begehung einer terroristischen Straftat sowie die Anwerbung und Ausbildung für terroristische Zwecke, wenn diese Handlungen rechtswidrig und vorsätzlich begangen werden, als Straftaten eingestuft werden. Nach Artikel 9 sind die Vertragsparteien überdies verpflichtet, ergänzende Straftatbestände zu den in Artikel 5 bis 7 genannten einzuführen.

- **Übereinstimmung mit anderen Politikbereichen und Zielen der Europäischen Union**

Der Vorschlag steht im Einklang mit der EU-Strategie und dem Aktionsplan zum Thema Radikalisierung und Anwerbung. Er aktualisiert und ergänzt den Rechtsrahmen der EU im Bereich der Terrorismusbekämpfung und achtet die Charta der Grundrechte der Europäischen Union [ABl. C 364 vom 18.12.2000, S. 1].

Maßnahmen zur Terrorismusbekämpfung müssen mit dem Schutz der Menschenrechte und Grundrechte einhergehen. Dieser Vorschlag betrifft Fragen, die sich im Grenzbereich zwischen der rechtmäßigen Ausübung von Freiheitsrechten wie der Meinungs-, Versammlungs- oder Religionsfreiheit und kriminellem Verhalten bewegen. Bei seiner Ausarbeitung wurde daher den Menschenrechten und Grundfreiheiten besondere Beachtung geschenkt. Die Beschränkungen des Rechts auf freie Meinungsäußerung durch den neuen Straftatbestand der öffentlichen Aufforderung zur Begehung einer terroristischen Straftat sind mit Artikel 10 EMRK vereinbar.

2. ANHÖRUNG VON INTERESSIERTEN KREISEN UND FOLGENABSCHÄTZUNG

- **Anhörung von interessierten Kreisen**

Anhörungsmethoden, angesprochene Sektoren und allgemeines Profil der Befragten

Die Kommission gab 2006 drei verschiedene Fragebögen aus: einen Fragebogen an die Mitgliedstaaten (26. Juni 2006), einen Fragebogen an die Medien, betroffenen Wirtschaftszweige und die Zivilgesellschaft, nationale, europäische und internationale NRO, die sich mit Menschenrechtsfragen befassen, Rechtsanwaltskammern, Verlagshäuser, Sendeunternehmen und Journalistenverbände, Internetanbietern, Telekommunikationsunternehmen und andere relevante Wirtschaftszweige (20. November 2006) sowie einen Fragebogen an Europol, Cepol und Eurojust (11. Dezember 2006). Darüber hinaus fanden Gespräche und Zusammenkünfte mit Vertretern der europäischen Medien und Internetanbieter statt. Am 20. März 2007 schließlich kamen auf einer Konferenz Vertreter der Mitgliedstaaten, von Europol sowie Eurojust und Cepol zusammen, um die Ergebnisse aus den Fragebögen zu erörtern und sich Gedanken darüber zu machen, wie der Missbrauch des Internets für terroristische Zwecke unterbunden werden kann.

Zusammenfassung der Antworten und Art ihrer Berücksichtigung

Die Antworten auf die drei Fragebögen sind in den Anhängen I, II und III der Folgenabschätzung, die diesem Vorschlag beigefügt ist, zusammengefasst.

Auf der Konferenz vom 20. März 2007 bestätigte sich, dass für eine Änderung des Rahmenbeschlusses zur Terrorismusbekämpfung durch die Aufnahme neuer Straftatbestände (öffentliche Aufforderung zur Begehung einer terroristischen Straftat, Anwerbung und Ausbildung für terroristische Zwecke, einschließlich über das Internet) eine ausreichende Unterstützung vorhanden ist, soweit die Kriminalisierung nicht über das im Europaratsübereinkommen zur Terrorismusverhütung festgelegte Maß hinausgeht.

Bei dem vorliegenden Vorschlag handelt es sich um eine ausgewogene Regelung, in die die Ergebnisse der drei Fragebögen und die in der Konsultation geäußerten Meinungen eingeflossen sind und die sich auf die im Anhang beigefügte Folgenabschätzung stützt. Die neuen Straftatbestände entsprechen zudem denen im Europaratsübereinkommen zur Verhütung des Terrorismus. Auf diese Weise ist gewährleistet, dass der öffentlichen Aufforderung zur Begehung einer terroristischen Straftat sowie der Anwerbung und Ausbildung für terroristische Zwecke, einschließlich über das Internet, mit geeigneten rechtlichen Mitteln begegnet werden kann. Der Vorschlag steht voll im Einklang mit den Menschenrechten und lässt die Haftung der Diensteanbieter auf der Grundlage der E-Commerce-Richtlinie unberührt.

- **Einholung und Nutzung von Expertenwissen**

Externes Expertenwissen war nicht erforderlich.

- **Folgenabschätzung**

Optionen:

1. Keine Änderung der bisherigen Politik (die Beibehaltung des Status quo erscheint angesichts des Übereinkommens des Europarats zur Verhütung des Terrorismus fragwürdig)
2. Internetanbietern wird untersagt, Zugang zu Inhalten zu gewähren, die auf eine öffentliche Aufforderung zur Begehung einer terroristischen Straftat, Anwerbung oder Ausbildung für terroristische Zwecke gerichtet sind

3. Durch geeignete Schulungen, eine leistungsfähige Ausrüstung und mit Hilfe von Experten – eventuell von der Kommission finanziert – werden die Strafverfolgungsbehörden in die Lage versetzt, sich mehr Kapazitäten und Fachkenntnisse anzueignen, mit denen sie dem Missbrauch des Internets für terroristische Zwecke entgegenwirken können
4. Die Mitgliedstaaten werden (im Wege einer politischen Erklärung) nachdrücklich aufgefordert, das Übereinkommen des Europarats zur Verhütung des Terrorismus zu unterzeichnen bzw. zu ratifizieren
5. Der Rahmenbeschluss zur Terrorismusbekämpfung wird geändert, um im Einklang mit dem Übereinkommen des Europarats zur Verhütung des Terrorismus Straftatbestände aufzunehmen, die die öffentliche Aufforderung zur Begehung einer terroristischen Straftat sowie die Anwerbung und Ausbildung für terroristische Zwecke, einschließlich über das Internet, unter Strafe stellen.

Nach sorgfältiger Prüfung der Folgen, die mit jeder einzelnen Option für die Sicherheit, die Wirtschaft und die Menschenrechte verbunden sind, und nach Abwägung ihrer Vor- und Nachteile erscheint eine Kombination der Optionen 3 und 5 die wirksamste Strategie zu sein, um den Missbrauch des Internets für terroristische Zwecke bei uneingeschränkter Achtung der Menschenrechte zu unterbinden.

Die Kommission hat die im Arbeitsprogramm aufgeführte Folgenabschätzung vorgenommen, die unter www.europa.eu abgerufen werden kann.

3. RECHTLICHE ASPEKTE

- **Zusammenfassung des Vorschlags**

Mit der vorgeschlagenen Änderung des Rahmenbeschlusses des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung sollen die einzelstaatlichen Vorschriften für die öffentliche Aufforderung zur Begehung einer terroristischen Straftat sowie für die Anwerbung und Ausbildung für terroristische Zwecke in der Weise angeglichen werden, dass diese Handlungen, auch wenn sie über das Internet begangen werden, überall in der EU unter Strafe gestellt werden und dass die für terroristische Straftaten geltenden Strafvorschriften sowie die Bestimmungen über die Haftung juristischer Personen, die gerichtliche Zuständigkeit und die Strafverfolgung auch für solche Handlungen gelten.

- **Rechtsgrundlage**

Artikel 29, Artikel 31 Absatz 1 Buchstabe e und Artikel 34 Absatz 2 Buchstabe b EUV.

- **Subsidiaritätsprinzip**

Handlungen der Europäischen Union unterliegen dem Subsidiaritätsprinzip.

Die Ziele des Vorschlags können von den Mitgliedstaaten aus folgenden Gründen nicht ausreichend verwirklicht werden:

Terrorismus ist heutzutage eindeutig global ausgerichtet. Die Verbreitung von Propaganda zur Mobilisierung und Rekrutierung von Sympathisanten und Aktivisten sowie die Verbreitung von Anleitungen und Online-Handbüchern für die Terrorismus-Ausbildung oder die Planung von Terroranschlägen über das Internet haben grenzübergreifenden, internationalen Charakter. Die Bedrohung ist international und international - zumindest zum Teil - muss auch die Reaktion darauf sein.

Die erfolgreiche Bekämpfung von Terrorismus und Cyberkriminalität auf EU-Ebene setzt ein abgestimmtes Vorgehen der Mitgliedstaaten sowie eine Zusammenarbeit auf internationaler Ebene voraus. Unterschiede in den Rechtsordnungen der Mitgliedstaaten erschweren sowohl ein abgestimmtes Vorgehen auf EU-Ebene als auch die Zusammenarbeit auf internationaler Ebene.

Die Ziele des Vorschlags können aus folgenden Gründen besser durch Maßnahmen der EU erreicht werden.

Es besteht eine klare Notwendigkeit, die Anstrengungen auf nationaler und EU-Ebene zur Bekämpfung des Terrorismus dem neuen Operationsmodus der Terroristen anzupassen. Durch die Ausweitung der derzeitigen gemeinsamen Terrorismus-Definition wird verhindert, dass sich Terroristen Unterschiede zwischen den nationalen Rechtsordnungen und Gesetzeslücken zunutze machen. Dies wird die Verfolgung grenzübergreifender krimineller Aktivitäten ganz erheblich erleichtern. Eine gemeinsame Basis, auf die sich alle Mitgliedstaaten stützen können, wird auch die Zusammenarbeit auf internationaler Ebene einfacher machen und die Position der EU in internationalen Gremien stärken.

Eine intensivere Zusammenarbeit in der EU und auf internationaler Ebene bewirkt eine effizientere Ermittlungsarbeit und Strafverfolgung und erhöht damit die Sicherheit.

Der Vorschlag steht daher mit dem Subsidiaritätsprinzip im Einklang.

- **Grundsatz der Verhältnismäßigkeit**

Der Vorschlag entspricht aus folgenden Gründen dem Grundsatz der Verhältnismäßigkeit.

Der Vorschlag geht nicht über das hinaus, was erforderlich ist und zudem einen Mehrwert auf EU-Ebene bewirkt. Als Rahmenbeschluss ist er für die Mitgliedstaaten hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.

Die E-Commerce-Richtlinie und die Richtlinie über die Vorratsspeicherung von Daten bleiben unverändert, so dass für Telekom-Betreiber oder Anbieter von Telekommunikationsdiensten keine neuen Pflichten entstehen. Mit dem Vorschlag ist für sie kein Aufwand in Form neuer Kooperationsmechanismen verbunden. Die vorhandenen Mechanismen im Rahmen der E-Commerce-Richtlinie und der Richtlinie über die Vorratsspeicherung von Daten werden lediglich in größerem Umfang genutzt werden. Die indirekten Kosten, die sich aus diesem Vorschlag ergeben, beschränken sich auf die zusätzliche Arbeitsbelastung, die mit der Einführung der neuen Straftatbestände einhergeht. In Anbetracht der Zahl der im Jahresdurchschnitt in der EU zu verzeichnenden Strafverfolgungsmaßnahmen wegen terroristischer Delikte dürften diese Kosten nicht sonderlich ins Gewicht fallen.

- **Wahl des Instruments**

Vorgeschlagenes Instrument: Rahmenbeschluss nach Artikel 34 Absatz 2 Buchstabe b EUV; andere Instrumente kommen nicht in Frage, da eine Angleichung der mitgliedstaatlichen Rechtvorschriften angestrebt wird.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Der Vorschlag hat keine Auswirkungen auf den EU-Haushalt.

2007/0236 (CNS)

Vorschlag für einen

RAHMENBESCHLUSS DES RATES

zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung

DER RAT DER EUROPÄISCHEN UNION -

gestützt auf den Vertrag über die Europäische Union, insbesondere auf Artikel 29, Artikel 31 Absatz 1 Buchstabe e und Artikel 34 Absatz 2 Buchstabe b,

auf Vorschlag der Kommission[1],

nach Stellungnahme des Europäischen Parlaments[2],

in Erwägung nachstehender Gründe:

(1) Terrorismus stellt einen der schwersten Verstöße gegen die universellen Werte der Würde des Menschen, der Freiheit, der Gleichheit und der Solidarität, der Achtung der Menschenrechte und der Grundfreiheiten dar, auf die sich die Europäische Union gründet. Er stellt zudem einen der schwersten Angriffe auf die Grundsätze der Demokratie und der Rechtsstaatlichkeit dar, die allen Mitgliedstaaten gemein sind und die der Europäischen Union zugrunde liegen.

(2) Der Rahmenbeschluss 2002/475/JI des Rates zur Terrorismusbekämpfung bildet die Grundlage der EU-Strategie zur Bekämpfung des Terrorismus. Mit der Einführung eines allen Mitgliedstaaten gemeinsamen Rechtsrahmens und insbesondere einer einheitlichen Definition terroristischer Straftatbestände konnte eine EU-Politik zur Terrorismusbekämpfung entwickelt und ausgestaltet werden, die auf der Achtung der Grundrechte und der Rechtsstaatlichkeit gründet.

(3) Die Bedrohung durch den Terrorismus hat in den letzten Jahren stark zugenommen und eine andere Qualität erhalten. Die Vorgehensweise von Terroristen und Sympathisanten hat sich verändert. An die Stelle organisierter, hierarchisch aufgebauter Strukturen sind halbautonome Zellen getreten, die nur locker miteinander verbunden sind. Solche Zellen stellen Verbindungen zwischen internationalen Netzen her und machen zunehmend von neuen Technologien, insbesondere dem Internet, Gebrauch.

(4) Das Internet wird zur Beeinflussung und Mobilisierung von lokalen Terrornetzen und Einzelpersonen in Europa eingesetzt und dient darüber hinaus als „virtuelles Trainingscamp“, indem es Informationen über Mittel und Methoden des Terrorismus verbreitet. Aktivitäten mit dem Ziel, öffentlich zur Begehung einer terroristischen Straftat aufzufordern oder Personen für terroristische Zwecke anzuwerben und auszubilden, haben sich angesichts der sehr niedrigen Kosten und Risiken vervielfacht.

(5) Dem Haager Programm zufolge kann Terrorismus unter uneingeschränkter Wahrung der Grundrechte nur dann wirksam verhütet und bekämpft werden, wenn sich die

1 [...]

2 [...]

Mitgliedstaaten nicht nur auf ihre eigene Sicherheit konzentrieren, sondern auch die Sicherheit der Union insgesamt im Auge haben.

(6) Im Aktionsplan zur Umsetzung des Haager Programms wird festgestellt, dass sich Terrorismus nur mit einer globalen Strategie bekämpfen lässt. Die Erwartungen, die die Bürger an die EU stellen, dürfen nicht ignoriert werden. Ebenso wenig kann die Union es sich leisten, diesen Erwartungen nicht zu entsprechen. Prävention und Krisenmanagement sind wesentliche Aspekte, um die Kapazitäten der Mitgliedstaaten zur Bekämpfung des Terrorismus zu stärken und erforderlichenfalls zu ergänzen. Hier gilt das Hauptaugenmerk dem Personalbedarf, der Risikoanalyse, dem Schutz anfälliger Infrastruktureinrichtungen und der Folgenbewältigung.

(7) Um zu dem allgemeineren politischen Ziel der Terrorismusprävention beizutragen und die Verbreitung von Material zu reduzieren, das Personen zu Terroranschlägen anstiften könnte, sollten Straftaten im Zusammenhang mit terroristischen Aktivitäten unter Strafe gestellt werden.

(8) In der Resolution 1624 des UN-Sicherheitsrats (2005) werden die Staaten aufgefordert, die notwendigen und geeigneten Maßnahmen im Einklang mit ihren völkerrechtlichen Verpflichtungen zu ergreifen, um die Anstiftung zur Begehung einer terroristischen Handlung oder terroristischer Handlungen gesetzlich zu verbieten und ein solches Verhalten zu verhindern. Dem Bericht des Generalsekretärs der Vereinten Nationen „Vereint gegen den Terrorismus – Empfehlungen für eine weltweite Strategie zur Bekämpfung des Terrorismus“ vom 27. April 2006 zufolge bietet die vorstehende Resolution die Grundlage dafür, die Anstiftung zu terroristischen Handlungen und die Rekrutierung, einschließlich über das Internet, unter Strafe zu stellen. In der Weltweiten Strategie der Vereinten Nationen zur Bekämpfung des Terrorismus (8. September 2006) haben die UN-Mitgliedstaaten beschlossen, Mittel und Wege zu erkunden, um die auf internationaler und regionaler Ebene unternommenen Anstrengungen zur Bekämpfung des Terrorismus in allen seinen Arten und Erscheinungsformen im Internet zu koordinieren.

(9) Im Übereinkommen des Europarats zur Verhütung des Terrorismus werden die Vertragsparteien verpflichtet, die öffentliche Aufforderung zur Begehung einer terroristischen Straftat sowie die Anwerbung und Ausbildung für terroristische Zwecke, wenn diese Handlungen rechtswidrig und vorsätzlich begangen werden, unter Strafe zu stellen.

(10) Die Definition terroristischer Straftaten einschließlich von Straftaten im Zusammenhang mit terroristischen Aktivitäten sollte in allen Mitgliedstaaten weiter angeglichen werden, um auch die öffentliche Aufforderung zur Begehung einer terroristischen Straftat sowie die Anwerbung und Ausbildung für terroristische Zwecke zu erfassen, wenn diese Handlungen vorsätzlich begangen werden.

(11) Für natürliche und juristische Personen, die öffentlich zur Begehung einer terroristischen Straftat aufgefordert oder Personen für terroristische Zwecke angeworben oder ausgebildet haben oder die für solche Handlungen haften, sind Strafen und Sanktionen vorzusehen, wenn diese Handlungen vorsätzlich begangen wurden. Diese Verhaltensweisen sollten in allen Mitgliedstaaten unter Strafe gestellt werden, unabhängig davon, ob sie über das Internet begangen werden.

(12) Es sollten zusätzliche Vorschriften zur gerichtlichen Zuständigkeit festgelegt werden, um eine wirksame Verfolgung der öffentlichen Aufforderung zur Begehung einer terroristischen Straftat sowie der Anwerbung und Ausbildung für terroristische

Zwecke sicherzustellen, wenn diese auf die Begehung einer terroristischen Straftat gerichtet sind oder zur Begehung einer terroristischen Straftat geführt haben, die in die gerichtliche Zuständigkeit eines Mitgliedstaats fällt.

(13) Da die Ziele der in Betracht gezogenen Maßnahmen einseitig durch die Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern aufgrund der erforderlichen Rechtsangleichung in der Europäischen Union besser auf EU-Ebene zu erreichen sind, kann die Europäische Union im Einklang mit dem Subsidiaritätsprinzip tätig werden. Dieser Rahmenbeschluss geht entsprechend dem Grundsatz der Verhältnismäßigkeit nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.

(14) Die Union achtet die in Artikel 6 Absatz 2 des Vertrags über die Europäische Union anerkannten und in der Charta der Grundrechte der Europäischen Union, insbesondere in den Kapiteln II und VI, niedergelegten Grundsätze. Dieser Rahmenbeschluss kann nicht dahin ausgelegt werden, dass er Grundrechte oder Grundfreiheiten wie das Recht auf Meinungs-, Versammlungs- und Vereinigungsfreiheit, das Recht auf Achtung des Privat- und Familienlebens einschließlich des Rechts auf Achtung des Brief- und Fernmeldegeheimnisses schmälert oder behindert.

(15) Bei der öffentlichen Aufforderung zur Begehung einer terroristischen Straftat sowie der Anwerbung und Ausbildung für terroristische Zwecke handelt es sich um vorsätzliche Straftaten. Dieser Rahmenbeschluss kann daher nicht dahin ausgelegt werden, dass er die Verbreitung von Informationen für Wissenschafts-, Forschungs- oder Berichtszwecke schmälert oder behindert. Die Äußerung radikaler, polemischer oder kontroverser Ansichten in einer öffentlichen Diskussion über sensible politische Themen einschließlich Terrorismus fällt nicht in den Anwendungsbereich dieses Rahmenbeschlusses und wird insbesondere nicht von der Definition der öffentlichen Aufforderung zur Begehung einer terroristischen Straftat erfasst -

HAT FOLGENDEN RAHMENBESCHLUSS ANGENOMMEN:

Artikel 1

Der Rahmenbeschluss vom 13. Juni 2002 zur Terrorismusbekämpfung wird wie folgt geändert:

(1) Artikel 3 erhält folgende Fassung:

„Artikel 3
Straftaten im Zusammenhang mit terroristischen Aktivitäten

1. Im Sinne dieses Rahmenbeschlusses gelten folgende Begriffsbestimmungen:

   (a) „Öffentliche Aufforderung zur Begehung einer terroristischen Straftat“: das öffentliche Verbreiten oder sonstige öffentliche Zugänglichmachen einer Botschaft mit dem Vorsatz, zur Begehung einer unter Artikel 1 Absatz 1 Buchstaben a bis h aufgeführten Handlung anzustiften, wenn dieses Verhalten, unabhängig davon, ob dabei terroristische Straftaten unmittelbar befürwortet werden, die Gefahr begründet, dass eine oder mehrere solcher Straftaten begangen werden könnten;

   (b) „Anwerbung für terroristische Zwecke“: eine andere Person dazu zu bestimmen, eine Handlung im Sinne von Artikel 1 Absatz 1 oder Artikel 2 Absatz 2 zu begehen;

(c) „Ausbildung für terroristische Zwecke“: die Unterweisung in der Herstellung oder im Gebrauch von Sprengstoffen, Feuer- oder sonstigen Waffen oder schädlichen oder gefährlichen Stoffen oder die Unterweisung in anderen spezifischen Methoden oder Verfahren mit dem Ziel, eine Handlung im Sinne von Artikel 1 Absatz 1 zu begehen, in Kenntnis der Tatsache, dass die vermittelten Fähigkeiten für diesen Zweck eingesetzt werden sollen.

2. Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, damit folgende vorsätzliche Handlungen als Straftaten im Zusammenhang mit terroristischen Aktivitäten eingestuft werden:

(a) öffentliche Aufforderung zur Begehung einer terroristischen Straftat;

(b) Anwerbung für terroristische Zwecke;

(c) Ausbildung für terroristische Zwecke;

(d) schwerer Diebstahl mit dem Ziel, eine der in Artikel 1 Absatz 1 aufgeführten Handlungen zu begehen;

(e) Erpressung mit dem Ziel, eine der in Artikel 1 Absatz 1 aufgeführten Handlungen zu begehen;

(f) die Ausstellung gefälschter Verwaltungsdokumente mit dem Ziel, eine der in Artikel 1 Absatz 1 Buchstaben a bis h und in Artikel 2 Absatz 2 Buchstabe b aufgeführten Handlungen zu begehen.

3. Für die Strafbarkeit einer Handlung nach Absatz 2 ist es nicht erforderlich, dass tatsächlich eine terroristische Straftat begangen wird.“

(2) Artikel 4 Absatz 2 erhält folgende Fassung:

„Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, damit der Versuch der Begehung einer Straftat nach Artikel 1 Absatz 1 und Artikel 3 mit Ausnahme des Besitzes nach Artikel 1 Absatz 1 Buchstabe f und der Straftaten nach Artikel 1 Absatz 1 Buchstabe i und Artikel 3 Absatz 2 Buchstaben a bis c unter Strafe gestellt wird.“

(3) In Artikel 9 wird folgender Absatz 1a eingefügt:

„1a. Jeder Mitgliedstaat begründet seine Gerichtsbarkeit über die in Artikel 3 Absatz 2 Buchstaben a bis c genannten Straftaten, wenn es Ziel oder Ergebnis der Straftat war, eine Straftat im Sinne des Artikels 1 zu begehen und diese Straftat nach den Kriterien in Absatz 1 Buchstaben a bis e seiner Gerichtsbarkeit unterliegt.“

Artikel 2

1. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um diesem Rahmenbeschluss vor dem [31. Dezember 2008] nachzukommen.

2. Die Mitgliedstaaten teilen dem Generalsekretariat des Rates und der Kommission vor dem [31. Dezember 2008] den Wortlaut der Bestimmungen mit, mit denen sie die sich aus diesem Rahmenbeschluss ergebenden Verpflichtungen in ihr nationales Recht umgesetzt haben. Auf der Grundlage eines anhand dieser Angaben erstellten Berichts sowie eines Berichts der Kommission überprüft der Rat vor dem [31. Dezember 2009], inwieweit die Mitgliedstaaten den Bestimmungen dieses Rahmenbeschlusses nachgekommen sind.

Artikel 3

Dieser Rahmenbeschluss tritt am Tag seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Geschehen zu Brüssel am

Im Namen des Rates
Der Präsident

COUNCIL OF THE EUROPEAN UNION

Brussels, 13 November 2007

Interinstitutional File: 2007/0236 (CNS)

14960/07
ADD 1

CATS 122
DROIPEN 104

PROPOSAL

from:	European Commission
dated:	12 November 2007
Subject:	COMMISSION STAFF WORKING DOCUMENT Accompanying document to the proposal for a COUNCIL FRAMEWORK DECISION amending Framework Decision 2002/475/JHA on combating terrorism IMPACT ASSESSMENT

Delegations will find attached a proposal from the Commission, submitted under a covering letter from Mr Jordi AYET PUIGARNAU, Director, to Mr Javier SOLANA, Secretary-General/High Representative.

Encl.: SEC(2007) 1424

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 6.11.2007
SEC(2007) 1424

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

Proposal for a

COUNCIL FRAMEWORK DECISION

amending Framework Decision 2002/475/JHA on combating terrorism

IMPACT ASSESSMENT

{COM(2007) 650 final}
{SEC(2007) 1425}

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Modern information and communication technologies play an important role in the development of the threat which is currently represented by terrorism: they may serve as a means of dissemination of propaganda aiming at mobilisation and recruitment as well as instructions and online manuals intended for training or planning of attacks, addressed at current and potential supporters.

The Internet, in particular, may serve as one of the principal boosters of the processes of radicalisation and recruitment: it is used to inspire and mobilise local networks and individuals in Europe and also serves as a source of information on terrorist means and methods, thus functioning as a 'virtual training camp'. The dissemination of terrorist propaganda and terrorist expertise through the Internet has therefore empowered terrorists, making the terrorist threat grow. Moreover, the importance of such dissemination can only be expected to increase, taking into consideration the fast growing number of users that will make the Internet an even more vital element of modern society than it is today.

Law enforcement authorities are presently in a difficult position to contain the spiral of violent radicalisation and easier terrorist attacks deriving from the dissemination of terrorist propaganda and terrorist expertise, especially through the Internet. The difficulties stem from insufficient legislation, from lack of capacity and expertise to cope with the volume and plurality of languages in which the terrorist propaganda and terrorist expertise are disseminated as well as from the nature of the Internet itself: its extra-territoriality together with the anonymity it provides seriously hinders the reaction of law enforcement authorities complicating both the removal of such contents from the Internet and the investigation and prosecution of those responsible for a website and its contents.

EU legislation does not explicitly cover public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism. Furthermore, it is doubtful that the Framework Decision on combating terrorism requires Member States to ensure that a significant part of the dissemination of messages through the Internet encouraging the commission of terrorist offences or providing for terrorist expertise, either accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment, is made punishable.

However, the Council of Europe Convention on the prevention of terrorism tackles the use of the Internet as a means for public provocation to commit terrorist offences, recruitment and training for terrorism. Furthermore, it contains conditions and safeguards ensuring the respect of human rights, in particular the right to freedom of expression. It will lead to the harmonisation of Member States' legislation in this area if all of them sign and ratify the Convention.

Adopting effective measures to counter the public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism, especially through the Internet, would contribute to the prevention of the development of a stronger and wider platform of terrorist activists and supporters. Such measures should include legal provisions to remedy the insufficient legislation referred to above as well as practical measures to enhance law enforcement authorities' capacities and expertise. These actions would help to reduce the risk of terrorist attacks and to diminish the possibilities for radicalisation and recruitment.

Any legislation in this field, dealing with issues which are on the border between the legitimate exercise of freedoms (such as freedom of expression, association or religion) and criminal behaviour would necessarily have a direct impact on fundamental rights. The establishment, implementation and application of criminalisation have to be carried out while respecting fundamental rights obligations. This also implies that all establishment, implementation and application of criminalisation is subject to the principle of proportionality, with respect to the legitimate aims pursued and to their necessity in a democratic society, excluding any form of arbitrariness or discriminatory or racist treatment[1].

The options identified to achieve this objective are:

1. No policy change (which is a debatable status quo because of the existence of the Council of Europe Convention on the prevention of terrorism).

2. Forbidding internet service providers to give access to material aiming at public provocation to commit terrorist offences, recruitment or training for terrorism.

3. Enhancing law enforcement authorities' capacities and expertise to counter the use of the Internet for terrorist purposes (through adequate training, the support of experts and efficient equipment, possibly financed by the Commission).

4. Urging Member States to sign and/or ratify the Council of Europe Convention on the prevention of terrorism (through a political statement).

5. Revising the Framework Decision on combating terrorism in order to introduce parallel offences to those foreseen under the Council of Europe Convention on the prevention of terrorism and make public provocation to commit terrorist offences, recruitment and training for terrorism, also via the Internet, punishable.

After careful examination of the impacts on security, economy and human rights of each of the options as well as weighing their advantages and drawbacks, the combination of options 5 and 3 appears to be the most effective policy to counter terrorist use of the Internet while fully respecting human rights.

The monitoring and evaluation of these measures would be ensured, concerning the revision of the Framework Decision on combating terrorism, by the evaluation of national implementation which generally applies to framework decisions, as foreseen under Article 11 of this instrument and, as regards the non-legislative measures of option 3, by Articles 13 and 15 of the Specific Programme Prevention of and Fight against crime. Article 13 details the monitoring of each of the actions financed under this programme and Article 15 sets out the rules for the evaluation of the programme itself.

---

[1] See the Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism, points 143-151.

1. SECTION 1: PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Background: organisation and timing, consultation and expertise

The Commission Legislative and Work Programme for 2007 includes a proposal for the revision of the Framework Decision of 13 June 2002 on combating terrorism (hereafter, "Framework Decision") in order to devise effective solutions towards fighting terrorist propaganda through various media and limiting the transmission of expertise, in particular on explosives and bomb making, for terrorist purposes.

In view of the eventual revision of the Framework Decision on combating terrorism, and taking into consideration the sensitivity of the subject because of real or perceived inroads in freedom of expression, a wide stock-taking exercise was launched in June 2006. The Commission issued three different questionnaires in 2006: a questionnaire to Member States on 26 June 2006; a questionnaire to national, European and international NGOs dealing with human rights issues, Human Rights bodies, Bar and Lawyers' associations, publishers, broadcasters and journalists' associations, internet service providers, telecommunication companies, and other relevant industry on 20 November 2006, and finally, a questionnaire to Europol, Cepol and Eurojust on 11 December 2006. In addition, conversations and meetings were held with representatives of European media and internet service providers. These included, in particular, the intervention of the Commission at the Corporate Affairs Group Meeting of the European Publishers Association on 19 September 2006 as well as a the meeting with the representatives of the European Federation of Magazine Publishers, the European Publishers Council, the European Newspaper Publishers' Association and the Association of Commercial Television in Europe on 10 October 2006.

In addition, a conference was held on 20 March 2007 in order to bring together Member States, Europol, Eurojust and Cepol, present the results of the questionnaires and discuss possible solutions to fight the use of the internet for terrorist purposes. The focus of the discussion was the eventual revision of the Framework Decision on combating terrorism in view of including explicit provisions on public provocation to commit a terrorist offence, recruitment for terrorism and training for terrorism comparable to those included in the Council of Europe Convention on the Prevention of Terrorism.

Besides the data obtained throughout the consultation process, various other information sources have been taken into account, namely the Report of the Secretary-General of the United Nations "Uniting against terrorism: recommendations for a global counter-terrorism strategy" of 27 April 2006[2], reports of the General Intelligence and Security Service of the Netherlands as well as of its National Coordinator for counter-terrorism[3], the EU Terrorism

---

2 Report of the Secretary-General of the United Nations "Uniting against terrorism: recommendations for a global counter-terrorism strategy" of 27 April 2006, Sixtieth session Agenda items 46 and 120, A/60/825 section C "Denying access to recruits and communication by countering terrorist use of the internet", p. 12, http://www.un.org/unitingagainstterrorism/sg-terrorism-2may06.pdf.

3 Annual Report 2005 of the General Intelligence and Security of the Netherlands, http://www.aivd.nl/contents/pages/81211/aivd_annual_2005.pdf and the 2006 report of the same body "Violent Djihad in the Netherlands, current trends in the Islamist terrorist threat", www.fas.org/irp/world/netherlands/violent.pdf. The 2006 report "Djihadis and the Internet" of the National Coordinator for counter-terrorism, http://english.nctb.nl/publications/reports/nctb/.

Situation and Trend Report 2007 of Europol[4] –as well as studies and articles from research centres, such as the Canadian Centre of Intelligence and Security Studies[5], and from scholars, including Maura Conway[6], Johnny Ryan[7], Gabriel Weimann[8], Bruce Hoffman[9], Hanna Rogan[10] and Alfonso García Merlos[11]. Additionally, this impact assessment takes stock of the first and second evaluation reports of the Commission on the implementation of the Framework Decision on combating terrorism[12], the explanatory report to Council of Europe Convention on the Prevention of Terrorism[13], and publications including "Apologie du terrorism and incitement to terrorism" by the Council of Europe[14], "Droit pénal comparé spécial"[15] and "Grunderfordernisse einer Regelung des Allgemeinen Teils"[16]. It also reflects

---

4 EU Terrorism Situation and Trend Report of Europol 2007, http://www.europol.europa.eu/index.asp?page=news&news=pr070410.htm.

5 "Tendances en terrorisme - L'usage d'Internet à des fins terroristes" http://www.csis-scrs.gc.ca/fr/itac/itacdocs/2006-2.pdf.

6 Several publications of this author have been used for the elaboration of this impact assessment. Among them "Terrorism and the Internet: new media-new threat?", Parliamentary Affairs Vol. 59 No. 2, 2006, Advance Access Publication 10 February 2006, http://pa.oxfordjournals.org/cgi/reprint/59/2/283 and "Terrorist use of the Internet and fighting back", www.oii.ox.ac.uk/research/cybersafety/extensions/pdfs/papers/maura_conway.pdf. In addition, Ms. Conway intervened in the conference organised on 20 March 2007 in the context of the impact assessment of the proposal, offering highly relevant expertise.

7 His study, "Countering Militant Islamist radicalisation on the Internet: a user driven strategy to recover the web", Institute of European Affairs 2007, has been especially useful concerning the analysis of technical solutions to the spread of violent radicalisation through the Internet.

8 One of the most influential authors in the area of the use of the Internet for terrorist purposes, his studies "Terror on the Internet: the new arena, the new challenges", Washington, D.C.: U.S. Institute of Peace Press 2006, and "www.terror.net - How modern terrorism uses the Internet", http://www.usip.org/pubs/specialreports/sr116.pdf, have been taken into account in the elaboration of this impact assessment.

9 His study, "The use of the Internet by Islamic extremists", http://www.rand.org/pubs/testimonies/2006/RAND_CT262-1.pdf, analyses very eloquent cases of the use of the Internet for terrorist purposes.

10 Her study, "Djihadism online – A study of how Al-Quida and radical Islamist groups use the Internet for terrorist purposes", http://rapporter.ffi.no/rapporter/2006/00915.pdf, constitutes an exceptional insight on the online Djihad.

11 "Internet como instrumento para la Djihad", Araucaria Revista Iberoamericana de Filosofía, Política y Humanidades. Año 8, Nº 16 Segundo semestre de 2006. ISSN 1575-6823 http://alojamientos.us.es/araucaria/nro16/ideas16_5.htm, has also been relevant in the elaboration of this impact assessment.

12 Concerning the first evaluation, the relevant documents are Report from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on combating terrorism - COM(2004) 409, 8.6.2004 and Commission staff working paper annex to the Report from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on combating terrorism - SEC(2004) 688, 8.6.2004. The relevant documents concerning the second evaluation are still to be published.

13 The explanatory report, http://conventions.coe.int/Treaty/EN/Reports/Html/196.htm, does not constitute an instrument providing an authoritative interpretation of the Convention, although it may serve to facilitate the application of the provisions contained therein.

14 "Apologie du terrorisme and incitement to terrorism", Council of Europe publishing, F-67075 Strasbourg Cedex, collects and analyses information received from the Member States in view of the elaboration of the Council of Europe Convention on the Prevention of Terrorism. In particular, it deals with a relatively new phenomenon: the public expression of praise, justification and other forms of support for terrorism and terrorists, which it refers to as "apologie du terrorisme" and "incitement to terrorism".

15 "Droit pénal comparé spécial, Dalloz, 2002, by Jean Pradel.

the legal expertise provided for by Erling Johannes Husabø, Professor of criminal law at the University of Bergen (Norway).

1.2. The Impact Assessment Board

On 20 July 2007, the Impact Assessment Board of the European Commission delivered an opinion regarding a preliminary version of this Impact Assessment report. In the opinion, the Board in brief stated:

(1) The IA needs to develop further the problem definition and explain gaps and differences in Member States' current legislation.

(2) The value added of a new EU initiative vis-à-vis the Convention of Council of Europe needs to be better demonstrated.

(3) The objectives of the proposal need to be clarified, particularly the relation between enabling easier tracking down of terrorists and limiting the terrorist propaganda.

(4) The impacts on fundamental rights should include positive indirect impacts on right to life, right to respect for physical and mental integrity, etc.

(5) The reasoning for discarding Option 2 could be developed further, expanding the discussion on (cost-) efficiency of this option, advantages and disadvantages of using currently available technologies.

The present version of the Impact Assessment report has been significantly redrafted, with a view to taking these recommendations fully into account. Additional information and modifications have been introduced to this end in many of its sections and an additional section has been created (Section 6.3. summary table: check list of benefits). As regards the need to develop further the gaps and differences in Member States' current legislation, the information is however limited by the number of Member States that replied to the Commission's questionnaire –eighteen- as well as by the completeness of the replies. The recommendation has in this case been followed to the possible extent.

---

[16] "Grunderfordernisse einer Regelung des Allgemeinen Teils", in "Wirtschaftsstrafrecht in der Europäischen Union", (Rechtsdogmatik- Rechtsvergleich-Rechtspolitik), by Klaus Tiedemann (ed.) Carl Heymanns Verlag KG. München, 2001.

1.3. State of play: Existing policy documents and legal instruments

1.3.1. Policy documents

At international level, there are already a number of international policy documents adopted by the United Nations, the OSCE and the G8 which deal with the use of the Internet for terrorist purposes. The following (non-exhaustive) examples can in particular be mentioned.

1. The United Nations Security Council resolution 1624 (2005) calls upon States to take measures that are necessary and appropriate, and in accordance with their obligations under international law, to prohibit by law incitement to commit a terrorist act or acts and to prevent such conduct;

2. The Report of the Secretary-General of the United Nations "Uniting against terrorism: recommendations for a global counter-terrorism strategy" of 27 April 2006, A/60/825 whose section C "Denying access to recruits and communication by countering terrorist use of the internet" interprets the abovementioned resolution as providing for a basis for the criminalisation of incitement to terrorist acts and recruitment, including through the Internet;

3. The United Nations Global Counter-Terrorism Strategy mentions in its point II (12) that the Member States of the UN resolve to "work with the United Nations, with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law, to explore ways and means to:

   coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet, and;

   use the Internet as a tool for countering the spread of terrorism, while recognising that States may require assistance in this regard."

6. The commitment by the G8 Summit (St. Petersburg, Russian Federation, 16 July 2006), to effectively counter attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists;

7. Decision No. 7/06 "Countering the use of the Internet for Terrorist Purposes" of the Ministerial Council of the OSCE, of 5 December 2006, to intensify action by the OSCE and its participating States, notably by enhancing international co-operation on countering the use of the Internet for terrorist purposes.

At EU level, the Communication "Terrorist recruitment - Addressing the factors contributing to violent radicalisation"[17] was an initial contribution to an EU Strategy and Action Plan on Radicalisation and Recruitment which was adopted by the JAI December 2005 Council as was foreseen by the Hague Program. This policy document identified various existing EU policies that could play an important role in addressing the problem, including broadcasting

[17] Communication from the Commission to the European Parliament and the Council entitled "Terrorist recruitment - Addressing the factors contributing to violent radicalisation" of 21 September 2005 - COM(2005) 313.

media and the Internet. The Revised Radicalisation and Recruitment Action Plan of the Council of the European Union, in its Paragraph 44 notes that "the Union should promote full implementation of UNSCR 1624 (2005) and use in this context its external relations policy to encourage third states not to allow the transmission through satellite channels or other media, of messages that contain hate speech or incite terrorist violence"[18].

Furthermore, the Communication "Towards a general policy on the fight against cyber crime"[19] formulates a general policy on the fight against cyber crime at EU level, including incitement to terrorist acts and glorification of terrorism. It also identifies the problem of the growing number of illegal content sites that are accessible in Europe[20]. In order to fight illegal content, the actions envisaged by the Communication include the promotion of dialogue as well as developing EU-level voluntary agreements and conventions between public authorities and private operators, especially Internet service providers[21].

1.3.2. Legal instruments

Within the European Union, the main legal instrument to be mentioned is the Council Framework Decision on combating terrorism[22]. This instrument approximates the definition of terrorist offences in all Member States and ensures that penalties and sanctions are provided for natural and legal persons having committed or being liable for such offences, which reflect their seriousness. In addition, this instrument set up the cases in which Member States are obliged to take jurisdiction over terrorist offences so that they can be efficiently prosecuted and includes specific measures with regard to protection of and assistance to victims of terrorist offences because of their vulnerability.

In particular, its Article 4 states that inciting, aiding or abetting terrorist offences should be made punishable by the Member States and its Article 2 requires Member States to hold criminally liable those directing a terrorist group or participating in its activities. The scope of these provisions vis-à-vis the dissemination of terrorist propaganda and terrorist expertise in so far as they amount to public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism, in particular through the Internet, will be carefully studied and discussed below.

At international level, the main legal instrument to be mentioned in this context is the Council of Europe Convention on the prevention of terrorism of 2005, which entered into force on 1 June 2007. All Member States of the European Union have signed this Convention, with the exception of the Czech Republic and Ireland whereas only Bulgaria, Denmark, Romania and Slovakia have ratified it so far[23]. This should however not be understood as reluctance since ratification procedures are underway and the final text of the Convention reflects a very fine

---

18 See Revised Radicalisation and Recruitment Action Plan Doc. 16530/1/06 REV 1 ENFOPOL 218 COTER 35.

19 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions "Towards a general policy on the fight against cyber crime" of 22 May 2007 - COM(2007) 267.

20 Communication referred to above in footnote 19, p. 3.

21 Communication referred to above in footnote 19, p. 10.

22 Other relevant EU legal instruments are studied in Section 2.5.3.

23 See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=196&CM=8&DF=5/16/2007&CL=ENG to check exact situation regarding signatures and ratifications.

balance and broad consensus obtained after extensive work, including consultations and negotiations. According to this Convention, parties must adopt the necessary measures to establish public provocation to commit a terrorist offence, recruitment for terrorism and training for terrorism, when committed unlawful and intentionally, as criminal offences under their domestic law.

Although these provisions do not explicitly refer to the commission of such offences via the Internet, they are in fact applicable irrespective of whether they are committed over the Internet or not, as the explanatory report to the Convention clarifies. These provisions, therefore, cover terrorist propaganda and dissemination of bomb-making and other terrorist expertise through the Internet as long as they amount to public provocation to commit a terrorist offence, recruitment or training for terrorism as defined in the Convention.

In addition, the instrument contains conditions and safeguards (i.e. Article 12) ensuring the respect of human rights, in particular the right to freedom of expression.

2. SECTION 2: DEFINITION OF THE PROBLEM

2.1. What is the issue or the problem that may require action?

2.1.1. The increasing dissemination of propaganda as well as bomb-making and other expertise for terrorist purposes, especially through the Internet

"Since the advent of the printing press using industrial age technologies in the 19th century, terrorists and extremist movements have employed every available mass communication technology"[24]. Yet, the use of media by modern terrorism nowadays is not comparable with that preceding the widespread use of the Internet and other new media technologies. At that time, in order to reach a wide audience and gain publicity for their cause, terrorists were obliged to draw the attention of conventional media and conditioned to the presentation of the facts made by these. The arrival of new media technologies represents a turning point: terrorists are no longer reliant on intermediaries to interpret their deeds. They now have the ability to tell their own stories via their websites and television stations. The level of editorial control afforded to terrorists by their access to new media technologies has substantially empowered them[25].

However, the dramatic change stemming from the access of terrorists to new technologies goes far beyond allowing them to spread their views among large audiences, particularly when it comes to the Internet. Actually, more worrying than disinformation reaching public opinion is the propaganda aiming at mobilisation and recruitment as well as the dissemination of instructions and online manuals intended for training or planning of attacks, addressed at current and potential sympathisers.

This concern cannot but increase when the dimensions of the phenomenon are taken into account. Websites, chat-forums and blogs operated by terrorist groups and their supporters

---

24 See Terrorism and the Making of the 'New Middle East': New Media Strategies of Hizbollah and al Qaeda", by Maura Conway, p 3.

25 See Terrorism and the Making of the 'New Middle East': New Media Strategies of Hizbollah and al Qaeda", by Maura Conway, pp. 3-7.

have multiplied in the last years[26]. Studies and reports from scholars, research centres and international organisations including the United Nations as well as from national intelligence services coincide to point out its importance. As an illustrative example, the Report of the Secretary-General of the United Nations "Uniting against terrorism: recommendations for a global counter-terrorism strategy" of 27 April 2006, states[27]:

"Terrorist networks rely on communication to build support and recruit members. We must deny them this access, particularly by countering their use of the Internet — a rapidly growing vehicle for terrorist recruitment and dissemination of information and propaganda. In 1998, there were fewer than 20 terrorist websites. By 2005, that number was estimated by experts to have surged into the thousands. Indeed it seems that some major recent attacks drew support from content on the Internet."

The Internet is cheap, fast, easily accessible and has a practically global reach. All these advantages, highly appreciated by law-abiding citizens that benefit from the Internet in their daily lives, are also unfortunately exploited by terrorists, who have perfectly understood the potential of the Internet as a tool to spread propaganda aiming at mobilisation and recruitment as well as to provide for instructions and manuals intended for training or planning of attacks at very low risk and cost. The Internet can be regarded as the largest platform for relatively anonymous public comments, where expression of radical opinions is unhampered by social control or risk of persecution. This explains why terrorists have taken to the Internet with such alacrity.

An example that illustrates the priority that terrorists place upon communication is the fact that in 1998 Al-Qaeda established four departments to conduct affairs in military, finance, Islamic study and media matters. For this last department, the Internet was a particularly important tool.

No form of terrorism ignores the importance of communication nor renounces to exploit the Internet[28]. However, it should be noted that Islamist terrorism[29] is particularly active in this field. Its activists and supporters produce high quality material and favour an inter-active use of the web which has proven very effective to fuel radicalisation and recruitment. Furthermore, its de-centralised structure perfectly fits into the web allowing Islamist terrorism to exploit the Internet to a further extent than forms of terrorism operating through highly structured and hierarchical groups.

---

26 Reports and studies coincide in the quick multiplication of these websites, estimating that nowadays there are over 5 000 of them. They also highlight their increasing sophistication, including the use of several languages as well as audiovisual material of high quality. An important aspect in the evolution of the terrorist use of the Internet is the increasing importance of the interaction through chat-forums and blogs.

27 See the Report of the Secretary-General of the United Nations "Uniting against terrorism: recommendations for a global counter-terrorism strategy" of 27 April 2006, Sixtieth session Agenda items 46 and 120, A/60/825 section C "Denying access to recruits and communication by countering terrorist use of the internet", p 12, http://www.un.org/unitingagainstterrorism/sg-terrorism-2may06.pdf.

28 Furthermore, nowadays almost all active terrorist organisations maintain websites, and many maintain more than one website.

29 Islamist terrorism is defined under Europol's report TE-SAT 2007 referred to above, in footnote 3, title 3 "TE-SAT 2007 Methodology", pp. 9-12, as a type of terrorism motivated either in whole or in part by an extreme interpretation of Islam and where the use of violence is regarded by its practitioners as a divine duty or sacramental act.

A report of the General Intelligence and Security Service of the Netherlands[30] confirms that modern information and communication technologies play a crucial role in the development of the threat which is currently represented by Islamist terrorism. With a graphic example, the report compares the Internet with a turbo propelling the global violent Djihad[31] movement, stating that it is one of the principal boosters of the processes of radicalisation and recruitment. The report continues detailing the mobilising and training purposes for which the Internet is used by terrorists groups explaining that the radical and extremist messages spread via the Internet both inspire and mobilise local Djihadist networks and individuals in Europe. The Internet, the report adds, can also stimulate and accelerate the emergence of real and virtual networks, and serves as a source of information on terrorist means and methods, thus functioning as a ‘virtual training camp’.

The report notes that this is a relatively recent phenomenon and therefore the study of the influence of the Internet on the development of the Djihadist movement and the role of this medium in individual radicalisation and Djihadisation is still at an early stage. However, on the basis of a number of recent cases, the report continues, it is possible to draw some tentative conclusions on various aspects of the so-called virtualisation of violent Djihad: "Virtualisation means that the ideological and organisational development of Djihadist networks and individuals is increasingly taking place on or with the help of the Internet. This obviously involves the risk that sooner or later virtual threat will turn into the specific threat of an actual attack. The General Intelligence and Security Service of the Netherlands expects that this virtualisation trend in particular will be essential in the future threat against Europe and the Netherlands"[32].

Despite the existence of other means through which mobilisation, recruitment and training can occur, the effort into distributing information online, and cases of militant operations in which the Internet is known to have played an important role, leads to the conclusion that Internet represents an increasingly important instrument to fuel violent radicalisation and ease terrorist attacks. The Internet has therefore empowered terrorists, making the terrorist threat grow. Moreover, the importance of online terrorism can only be expected to increase, taking into consideration the fast growing number of users that will make the Internet even a more vital nerve in modern society than it is today.

However, it is important to clarify that the dissemination of terrorist propaganda aiming at mobilisation or recruitment and instruction or manuals intended for training or planning of attacks does not only take place online. The Internet has not eliminated traditional means of dissemination such as distributing printed material or exhibiting videos. Moreover, the web boosts and complements other methods of dissemination. In those countries or regions where the Internet is not so widespread, the access of one individual is enough to record audio or video files or copy documents containing terrorist propaganda or terrorist expertise that will be latter distributed or exhibited to those who do not have the means to go online. In this

---

30 Report of the General Security and Intelligence Service of the Netherlands, "Current trends in the Islamist terrorist threat", 2006, www.aivd.nl/contents/pages/65582/jihad2006en.pdf.

31 This study uses the concepts of "Djihad", "Djihadism" or "Djihadist" when it quotes papers, reports or studies previously elaborated. Otherwise, the term employed is "Islamist terrorism", in the sense of the definition of Europol's report TE-SAT 2007 referred to above, in footnote 30.

32 See the report mentioned above, footnote 23, pp. 43-44, www.aivd.nl/contents/pages/65582/Djihad2006en.pdf.

sense, the lack of access to the new technologies does not impede access to material originally posted online.

Europol's report TE-SAT 2007 analyses the situation of terrorism in the European Union specifying that 706 individuals were arrested in 2006 as terrorist suspects[33]. Islamist terrorism is examined in detail, including the importance of propaganda for this type of terrorism. A total of 340 persons were reported to have been arrested on Islamist terrorism related offences between October 2005 and December 2006[34]. Concerning propaganda, in general, 2006 saw a rise in the frequency of statements and communiqués by Islamist groups, especially Al-Quaeda[35].

The concepts of terrorist propaganda, terrorist expertise and dissemination

Terrorist propaganda and terrorist expertise in this impact assessment are not legal concepts, but cover a variety of acts. From the legal point of view, in accordance with the Council of Europe Convention on the prevention of terrorism, these acts are to be criminalised only in so far as they amount to public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism.

Terrorist propaganda in this impact assessment refers to a variety of contents. From glorification of suicide bombers as “martyrs” to open encouragement to join terrorism, including direct invitations to “kill the heretic” without forgetting the justification of terrorism[36] or the dissemination of images of brutal assassinations as a way to gain publicity for the terrorists cause or prove their power, increasing fear. Thus, this term covers terrorist propaganda for diverse purposes: mobilising, recruiting or fund-raising.

However, the scope of this notion is restricted by two requirements: first of all, the information transmitted should actually create the risk that one or more terrorist offences are committed or the risk of recruitment; secondly, the content should be disseminated for the purpose of contributing to terrorist activity.

Terrorist expertise in this impact assessment includes all sorts of materials, from brief military instruction manuals to comprehensive encyclopaedias such as the infamous “Encyclopaedia for the preparation of the Djihad”, in both written as well as audio-visual form. The concept also covers content such as how to produce home-made explosives and poisons or how to use weapons, as well as strategic information including instructions on how to carry out attacks, reconnaissance operations, hostage-taking or how to establish an underground organisation, without forgetting data on targets to help the planning and co-ordination of attacks.

Similarly to terrorist propaganda, the scope of terrorist expertise is restricted by two requirements: first of all, the information transmitted should be actually useful for the commission of one or more terrorist offences; secondly, the information should be transmitted with the purpose of contributing to terrorist activity.

---

33 Europol's report TE-SAT 2007, referred to above in footnote 3, p. 14.

34 See Europol's report TE-SAT 2007, referred to above in footnote 3, p. 19.

35 See Europol's report TE-SAT 2007, referred to above in footnote 3, p. 26.

36 See i.e. “Djihadism online – A study of how Al-Qaeda and radical Islamist groups use the Internet for terrorist purposes”, mentioned above, footnote 9, p. 15 and “The use of the Internet by Islamic extremists”, mentioned above, footnote 8, pp. 6-7.

Pointing out the intentional element in the transmission of terrorist expertise is particularly relevant. Actually, unintentional propaganda is quite difficult to imagine. However, transmitting expertise on bomb-making or the use of weapons may have a different purpose than contributing to terrorist activity. Sometimes, the author might even be unconscious of such a risk. Even information in governmental sites may constitute a significant help for terrorists. For example, the US Nuclear Regulatory Commission Office of Nuclear Security and Incident Response recently took more than 1,000 sensitive documents off line considering that they would provide clear and significant benefit to a terrorist planning an attack[37].

The element of "terrorist intent" would exclude the dissemination of material for scientific, academic or reporting purposes (or any other purpose that is not contributing to terrorist activity). It follows that the expression of radical, polemic or controversial views in the public debate on sensitive political questions, including on terrorism issues, as well as the dissemination, even consciously, of distorted information, does not amount to the dissemination of terrorist propaganda or terrorist expertise.

It should be noted that there are often mixed cases where the transmission of terrorist propaganda and expertise comes together: messages containing instructions for a terrorist attack often include a component of encouragement[38].

This study focuses on the study of online dissemination of terrorist propaganda and terrorist expertise through messages accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment, as a recent phenomenon of important consequences and huge dimensions. However, offline distribution of terrorist propaganda and terrorist expertise is also comprised in the concept of "dissemination" used in the impact assessment, which includes any form of distribution that makes available terrorist propaganda or terrorist expertise to the public, to a group of current or potential sympathisers or to pre-selected candidates for recruitment.

Dissemination in this impact assessment consists of making terrorist propaganda and terrorist expertise available to the public, to a group of current or potential sympathisers or to pre-selected candidates for recruitment, by any means either on or offline.

2.1.2. Insufficient legislation to tackle the increasing dissemination of terrorist propaganda and terrorist expertise

The analysis of EU and national legislation included in Annex IV explains in detail why existing legislation at EU and national level is insufficient. This analysis covers the Television without frontiers Directive, the Directive on electronic commerce and the Data retention Directive although it focuses on Criminal law, in particular, on the relevant provisions of the Framework Decision on combating terrorism – Articles 2 and 4 - as well as the relevant Criminal law in Member States.

---

37 See “Terrorist use of the Internet and fighting back”, by Maura Conway, pp. 14-15, www.oii.ox.ac.uk/research/cybersafety/extensions/pdfs/papers/maura_conway.pdf.

38 See i.e. the example of the website Ansar al-Muslimin cited by Hanna Rogan as a site that “recommended attacks in lunch areas, overhead walkways and traffic snarls, where westerns would be trapped in their vehicles” in “Jihadism online – A study of how Al-Qaeda and radical Islamist groups use the Internet for terrorist purposes”, mentioned above, p. 30.

2.1.2.1. Criminal law

As regards Criminal law, the analysis provided for in Annex IV offers the following conclusions:

1. It is doubtful that Article 4 of the Framework Decision requires Member States to ensure that the dissemination of messages through the Internet encouraging the commission of terrorist offences, either accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment, is made punishable.

The doubt stems from the fact that Article 4 does not include the obligation for Member States to ensure that attempts to incite others to commit terrorist offences are made punishable. In this sense, it could be defended that the provision only obliges Member States to incriminate incitement when at least one of the recipients of the message is actually incited. This would lead to the conclusion that Article 4 does not require Member States to make the dissemination of messages encouraging the commission of terrorist offences via the Internet itself punishable.

The first evaluation report on national implementation seems to confirm this interpretation concerning public dissemination (the case of messages accessible to anyone): it concluded that all Member States would be able to meet the terms of Article 4 through their national provisions on complicity and inchoate offences whereas only three Member States had submitted provisions dealing with public dissemination of messages encouraging the commission of terrorist offences.

2. It is doubtful that Article 4 of the Framework Decision requires Member States to ensure that the dissemination of messages through the Internet providing for terrorist expertise, either accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment, is made punishable.

Once again, the doubt stems from the fact that this provision does not include the obligation for Member States to ensure that the attempt of aiding or abetting others to commit terrorist offences is made punishable and it seems that the dissemination of the messages referred to above via the Internet should be qualified as an attempt.

3. It seems that Article 2 of the Framework Decision does not require Member States to ensure that a significant part of the dissemination of messages through the Internet encouraging the commission of terrorist offences, either accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment is made punishable.

Article 2 includes the requirement of contributing to the criminal activities of a terrorist group.. In this sense, it could be defended that messages accessible to anyone, restricted to members of a chat-forum or addressed to potential recruits fall out of the scope of Article 2. Concerning messages aimed at fund-raising or recruitment for a terrorist group, they seem to meet such requirement. However, these messages would actually constitute an attempt of fund-raising and recruitment and the criminalisation of attempt under Article 4 does not cover the attempt to commit offences related to terrorist groups.

4. It seems that Article 2 of the Framework Decision does not require Member States to ensure that a significant part of the dissemination of messages through the Internet providing for terrorist expertise, either accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment is made punishable, save in exceptional cases.

Once again, since Article 2 includes the requirement of contributing to the criminal activities of a terrorist group, it could be argued that the dissemination of terrorist expertise is not covered by Article 2 insofar as the recipients are undetermined (i.e. messages accessible to anyone or disseminated in a chat forum) or potential recruits.

6. Seventeen Member States that replied to the questionnaire have got or are adopting provisions addressing direct invitations to commit a specific terrorist offence through messages accessible to anyone (i.e. website), restricted (i.e. chat forum) and addressed to pre-selected candidates for recruitment.

Seventeen out of the eighteen Member States that answered the questionnaire have got or are adopting provisions addressing direct invitations to commit a specific terrorist offence under offences of "provocation", "instigation", "public incitement" etc. Additionally, eight Member States have got or will have provisions explicitly condemning glorification or approval of terrorist offences (and often of other crimes). Two Member States deal specifically with the denigration or humiliation of the victims. Two also refer to apology of terrorism or crime apology.

7. Nine Member States that replied to the questionnaire have got or are adopting provisions that explicitly cover the transmission of terrorism expertise which are applicable to either messages accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment.

8. Generally speaking, national provisions of Member States, although not harmonised, substantially cover the dissemination of terrorist propaganda and in some cases also terrorist expertise while the Framework Decision on combating terrorism stays behind. Furthermore, the European instrument already appears to be out-dated in the international context, where the Council of Europe[39] and the United Nations[40] have set the basis for further reaching national legislation.

Therefore, the analysis included in Annex IV leads to the conclusion that EU legislation does not fully cover the dissemination of terrorist propaganda and terrorist expertise - most Member States currently provide only for non-harmonised and partial legal solutions. In particular, the Framework Decision on combating terrorism does not require Member States

39 See the Council of Europe Convention on the Prevention of Terrorism, mentioned above.

40 The Report of the Secretary-General of the United Nations "Uniting against terrorism: recommendations for a global counter-terrorism strategy", interprets Security Council Resolution 1624 (2005) as providing for a basis for the criminalization of incitement to terrorist acts and recruitment, including through the Internet.

to ensure that the dissemination of messages containing terrorist propaganda or providing for terrorist expertise is made punishable save in exceptional cases.

Concerning national legislation, as explained above, seventeen Member States (out of eighteen that answered the questionnaire) currently provide for or are adopting legal solutions to tackle the dissemination of messages encouraging the commission of terrorist offences. Nevertheless, very different concepts are used, including "provocation", "instigation", "public incitement", "glorification", "approval" or "apology" and "denigration of the victims", which results in lack of clarity and sometimes obviously different scopes. In particular, it seems that in many cases indirect provocation is not covered. In consequence, the dissemination of messages encouraging persons to join a terrorist movement or to become a terrorist, without reference to a specific terrorist offence risks to remain unpunished. Concerning the dissemination of terrorist expertise, nine Member States (out of the eighteen that answered the questionnaire) have got or are adopting rules that can cover the dissemination of messages containing terrorist expertise. It follows that there is a security gap to be addressed and that harmonisation is required.

Lack of harmonisation and insufficient legislation in many Member States hinders prosecutions within the national territory as well as police and judicial co-operation with other Member States where the dissemination of terrorist propaganda and terrorist expertise have been made punishable. In this sense, Europol notes that the number of investigations into terrorist propaganda seems small compared to the amount of the propaganda circulating on the Internet[41]. It indicates that one of the reasons is the lack of legislation allowing for arrests or investigations[42]. Similarly Eurojust states that, in order to be able to fight adequately the use of the Internet for terrorist purposes, proper legislation would need to be enforced so that law enforcement authorities working on such cases are not hindered by a lack of legal provisions. This body notes that outlawing Internet websites supporting or displaying terrorist views would already be a good step forward[43].

This situation is expected to improve, since the signature and ratification of the Council of Europe Convention on the prevention of terrorism by a large number of Member States will address the problems of lack of harmonisation and legal loopholes identified at national level to a large extent. It will constitute a significant improvement in terms of security allowing law enforcement authorities to investigate the dissemination of terrorist propaganda and terrorist expertise throughout the European Union and hold terrorist activists and supporters behind such dissemination liable for public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism[44]. However, it does not appear as the optimal solution to the problem because of several reasons.

First of all, given the urgency of the problem, it would not be appropriate to wait for the process of signature and ratification by all Member States – as mentioned above two Member States have not even signed the Council of Europe Convention. Experience shows that ratification processes are usually lengthy and often extend over long periods of time. Secondly, framework decisions present important advantages vis-à-vis international conventions and treaties, namely the obligation of Member States to notify the

---

41 See Europol's report TE-SAT 2007, referred to above in footnote 3, p. 21.
42 See Europol's report TE-SAT 2007, referred to above in footnote 3, p. 21.
43 See Annex III.
44 See Section 5.1.1, security impact of option 1.

implementation measures adopted, the elaboration of an evaluation report on the correct and full implementation of Member States by the Commission, which is later assessed by the Council, and the fact that the European Court of Justice is entitled to deliver preliminary rulings[45].

In addition, if the new offences introduced by the Council of Europe Convention remain outside the Framework Decision on combating terrorism, such offences remain outside the benefits achieved through all prior harmonisation in the field of the fight against terrorism. This includes rules on penalties and jurisdiction as well as the automatic application of the European Arrest Warrant and other instruments linked to the Framework Decision on combating terrorism[46]. Given the importance of the phenomenon and the commitment of the European Union to the fight against terrorism, the EU arsenal of counter-terrorism measures should clearly also be applicable to public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism.

Moreover, it would create illogical discrepancies where, for example, producing a counterfeit passport to contribute to a terrorist plot would come under all EU harmonisation on counter-terrorism but not recruiting or training through the Internet, encouraging the commission of terrorist offences and even arranging the entrance of new recruits in a training camp. Similarly, those stealing sensitive data on public infrastructure in preparation of a terrorist attack that others plan to commit are now covered by the regime of the Framework Decision. However, those distributing the very same information through the Internet, and even accompanying it with instructions on how to perpetrate the attack, would not be covered by the Framework Decision.

Finally, the nature of the problem requires international co-operation and co-operation with internet service providers. The insufficiency of EU legislation incriminating the dissemination of terrorist propaganda and terrorist expertise leaves the European Union in a weak position to request their assistance. Once again, given the commitment of the European Union to the fight against terrorism, the European Union should not loose an opportunity to strengthen its position to seek the required co-operation with third countries and private sector (see section 5.5.1 security impact of section 5).

2.1.2.2. Non criminal law

Concerning EC instruments, the analysis included in Annex IV examines the Television without frontiers Directive, the Directive on electronic commerce and the Data retention Directive.

The conclusions of this analysis with respect to non-criminal law are the following:

1. The Television without frontiers Directive does not currently apply to the Internet and after its ongoing revision will only apply to a restricted portion of the content available on the internet. In addition, it does not directly outlaw the dissemination of terrorist propaganda and terrorist expertise but prohibits incitement to hatred. It follows that this instrument provides for a rather limited solution to tackle the dissemination of terrorist propaganda and terrorist expertise, especially through the Internet.

45 See section 5.5.1 security impact of option 5.
46 See section 5.5.1 security impact of option 5.

2. The Directive on electronic commerce allows law enforcement authorities to request internet service providers to remove from or disable access to a website. However, its application requires that the dissemination of terrorist propaganda or terrorist expertise is outlawed. In many Member States the dissemination of terrorist propaganda or terrorist expertise is not fully incriminated or forbidden, excluding the use of the co-operation channels foreseen under the e-commerce Directive.

3. The Data retention Directive allows law enforcement authorities to request to internet service providers the location and traffic data. Nevertheless, the data retention Directive only applies regarding serious crimes. It follows that the complete or partial lack of incrimination by many Member States excludes the request of data to service providers under the Data retention Directive.

Therefore, the analysis leads to the conclusion that the relevant EC legislation either will only very partially cover the dissemination of terrorist propaganda and terrorist expertise (Television without frontiers Directive) or requires that the behaviour is previously outlawed or made punishable in order to be applicable (Directive on electronic commerce and Data retention Directive respectively). As regards the two last instruments, the absence of relevant criminal law fully covering the dissemination of terrorist propaganda and terrorist expertise in many Member States referred to above plays an important role, limiting the use of such instruments.

Additionally, it should be noted that the investigation of the dissemination of terrorist propaganda and terrorist expertise and the prosecution of the terrorist activists and supporters behind it is currently impossible under all three instruments.

2.1.3. Practical difficulties of law enforcement authorities facing increasing dissemination of terrorist expertise and terrorist propaganda

Law enforcement authorities are currently in a difficult position to contain the spiral of violent radicalisation and ease of terrorist attacks deriving from the dissemination of terrorist propaganda and terrorist expertise, especially through the Internet. The difficulty does not only derives from the insufficient legislation referred to above, but also from practical difficulties such as the lack of capacities and expertise as well as the nature of the Internet itself: its extra-territoriality together with the anonymity it provides greatly complicates the investigation and prosecution of those using the web as a means to disseminate propaganda aiming at mobilisation and recruitment for terrorism, as well as to transmit bomb-making and other terrorist expertise.

2.1.3.1. Lack of law enforcement authorities' capacities and expertise

The volume and number or languages of the messages disseminating terrorist propaganda and terrorist expertise is huge. Law enforcement authorities and other services involved in the fight against terrorism (hereafter law enforcement authorities) lack of capacity and expertise: processing and interpreting the websites in question is an enormous time-consuming and

labour-intensive process, because of the quantity of the material[47] and the languages[48] in which the documents have been established.

2.1.3.2. The nature of the Internet itself

Concerning the difficulties stemming from the nature of the Internet itself, Europol notes that law enforcement agencies have difficulties in identifying individuals who spread Islamist terrorist propaganda on the Internet[49]. The virtual nature of the Internet knows no boundaries and together with its anonymity complicates the identification of those responsible of a website and its contents[50]. Besides high technical skills, assistance from internet service providers is often required to achieve the desired identification. However, it is extremely likely that the internet service providers whose assistance is needed are outside the Member State that carries out the investigation. Furthermore, in many cases they will be based outside the European Union. As regards the removal of the sites in question, the problem of extra-territoriality is equally present, since most of the websites containing terrorist propaganda and terrorist expertise are hosted by internet service providers based in third countries. In addition, the issue of the speedy re-apparition of websites that have been closed down must be considered: when a website is successfully removed from a host server, it reappears very easily under another name. It can also reappear outside the jurisdiction of the European Union, in order to avoid the eventuality of being closed down once more.

The success of both kinds of requests – obtaining data to identify the one responsible for the website and its contents or closing down the website itself - depends on the legislation in the State where the internet service provider is based, as well as on existing co-operation agreements between the requesting and the requested States. Currently, insufficient legislation in many Member States means that such co-operation is not even guaranteed within the European Union. Successful co-operation with third countries appears even more uncertain. Europol states that, considering that a wide range of terrorism related websites fall outside the jurisdiction of Member States, there is a need for a common European Union approach towards foreign States which, knowingly or not, are harbouring terrorism-related websites, in order to make them adopt or change their legislation[51]. However, such EU approach requires previous legal measures outlawing the dissemination of terrorist propaganda and terrorist expertise in all Member States.

This dimension of the problem, including technical difficulties and international co-operation issues is however not specific to the use of the Internet for terrorist purposes but shared by all content-related crimes. The Communication "Towards a general policy on the fight against cyber crime" has addressed this issue when referring to illegal content in a general sense[52].

2.2. Who is affected, in what ways, and to what extent?

Firstly, terrorists: characteristics of the Internet such as ease of access, global reach, speed, lack of regulation, dynamicity and interactivity, individual control, anonymity and reduced

---

47 As explained in footnote 24, reports and studies coincide in the quick multiplication of these websites, estimating that nowadays there are over 5 000 of them.

48 These include many non European languages.

49 See Europol's report TE-SAT 2007, referred to above in footnote 3, p. 21.

50 See Annexes II and III.

51 See Annex III.

52 Communication referred to above in footnote 19, pp. 3 and 10.

transaction costs, make of it a key tool for terrorists. It allows for spreading violent radicalisation and easing terrorist attacks at very low cost and risk. The Internet has therefore empowered terrorists.

Potential and current sympathisers are also affected: selected as potential recruits or financers through the Internet, they become the target of messages aiming at recruitment or fund-raising. Therefore, they are more easily accessible for recruiters that can multiply the number of targets, the frequency of contacts, and the volume of information supplied at very low cost and risk. Exposure of sympathisers to specifically targeted propaganda increases therefore the chances that more sympathisers become activists and supporters.

Citizens are generally concerned: since the use of the Internet for terrorist purposes contributes to fuel violent radicalisation and makes terrorist attacks easier, the dissemination of these contents through the Internet increases the terrorist threat and hinders security.

Internet service providers since their services are abused: internet service providers cannot monitor all information they host or give access to, because of its volume. Terrorist activists and supporters benefit from this circumstance and use the Internet to disseminate terrorist propaganda and recruitment without internet service providers noticing.

Finally, law enforcement authorities are logically affected: first of all, as explained above, they are in a difficult position to contain the spiral of violent radicalisation and easier preparation of terrorist attacks deriving from the dissemination of terrorist propaganda and terrorist expertise, especially through the Internet[53]. Secondly, because the resulting stronger and wider platform of activists and supporters amounts to a growing terrorist threat, which directly concerns law enforcement authorities in their task of preventing crimes and protecting citizens.

2.3. How would the problem evolve, all things being equal?

As hinted at above, the fast growing number of users will make the Internet in the future even a more vital infrastructure in modern society than it is today. Therefore, the importance of the online dissemination of terrorist propaganda and terrorist expertise can only be expected to increase and, with it, the role of the Internet as a key instrument to fuel violent radicalisation and make terrorist attacks easier. Terrorist propaganda and terrorist expertise will reach an even larger audience which will easily access messages providing for encouragement, justifications and expertise to perform a terrorist attack. The number of both supporters and activists is in consequence expected to rise, creating a stronger and wider platform which will amount to a growing terrorist threat. Helped by the Internet, terrorists will become even more de-centralised, be able to communicate and operate faster and become even more difficult to trace.

2.4. Does the EU have the power to act?

Given the scope and magnitude of the terrorist threat posed by the proliferation of the dissemination of terrorist propaganda as well as terrorist expertise through the Internet, a need to tackle this threat persists and is growing. Radicalisation, recruitment and training connected

---

53 For more detailed information on the difficulties of law enforcement authorities to cope the terrorist use of the Internet, see Annex III.

to the dissemination of terrorist propaganda and terrorist expertise have a global dimension and, in consequence, cannot be dealt with only at national level. The threat is international, and so must be at least a part of the answer. It is beyond any doubt that the fight against terrorism will continue to be most important at a national level, but there is a clear need to extend the current complementary efforts at national and EU level to the new modus operandi of terrorist groups referred to above.

The EU actions discussed in this impact assessment report will not go beyond what is required and what is adding value at the EU-level. The fight against terrorism, including the dissemination of terrorist propaganda and terrorist expertise through the Internet will also in the future primarily be a responsibility of Member States, and the scale of EU intervention will remain limited. However, the benefits of EU-level action in this field should not be underestimated. Operational law enforcement work against cross-border criminal activities would be considerably facilitated.. The intrinsic international and cross-border character of dissemination of terrorist propaganda and terrorist expertise through the Internet is proof enough that actions are needed both at international and at EU-level. This study will identify the need for appropriate measures at EU level. This action shall be understood in the context of both terrorist and cyber-crime EU policies, which require coordinated efforts of Member States as well as co-operation at an international level in order to achieve their aims. It should again be underlined that EU action in the field of dissemination of terrorist propaganda and terrorist expertise especially through the Internet will only be a supplement to national and other international policies. A reinforced EU coordination should mainly be regarded as a limited but nevertheless very important contribution to the national and global actions against terrorism and cyber crime.

The proportionality of the options analysed in this impact assessment will be carefully assessed so that it becomes clear whether or not they go beyond what is necessary to achieve the objectives described under section 3. The proportionality will be especially considered concerning the respect of human rights, since this impact assessment addresses issues that are on the borderline between the legitimate exercise of freedoms, such as freedom of expression, association or religion, the respect of fundamental rights and freedoms, and criminality. Those options which do not prove fully compliant with human rights and fundamental freedoms will have to be rejected.

Proportionality is also an element to be taken into consideration regarding the costs that the options assessed might entail for the private sector, in particular for internet service providers. Any action imposing a disproportionate burden on the private sector will therefore be discarded.

This report will assess, among other policy options, the adoption of a proposal for the revision of the Framework Decision on combating terrorism. The legal basis for this action would be the same as the legal basis for the adoption of the Framework Decision on combating terrorism itself: Articles 29, 31 (1) (e) and 34 (2) (b) TUE.

3. SECTION 3: OBJECTIVES

General objective: Countering the increasing dissemination of terrorist propaganda and terrorist expertise in particular through the Internet.

Effective measures should be adopted in order to make the Internet a more hostile environment for terrorists and reduce its contribution to mobilisation of terrorism supporters, recruitment and training for terrorism. Since the dissemination of terrorist propaganda and terrorist expertise, especially through the Internet, represents an increasingly important factor contributing to fuelling violent radicalisation and assisting in the preparation of terrorist attacks, adopting effective measures against such dissemination would contribute to prevent the development of a stronger and wider platform of terrorist activists and supporters. Such measures would therefore help to reduce the possibilities for radicalisation and recruitment as well as the risk of terrorist attacks.

In order to meet this goal, two operational and more specific objectives should be achieved.

1. Strengthening the legal framework to fight the dissemination of terrorist propaganda and terrorist expertise, especially through the Internet.

In order to contain the development of a stronger and wider platform of terrorist activists at European Union level, modern terrorism and its new modus operandi must be fought by the European Union with the same determination and strength as demonstrated in the fight against traditional terrorism. Law enforcement authorities must be clearly allowed to investigate the dissemination of terrorist propaganda and terrorist expertise, also through the Internet, and prosecute the terrorist activists and supporters behind such dissemination throughout the European Union. Furthermore, law enforcement authorities must benefit from all harmonisation that has already been achieved in the fight against terrorism and use co-operation instruments such as the European Arrest Warrant for these new forms of crime.

Therefore, the definition of terrorist offences, including offences linked to terrorist activities, should be further approximated in all Member States so that the dissemination of terrorist propaganda and terrorist expertise, also through the Internet, is punishable throughout the European Union. This would also allow a common EU approach towards foreign States whose co-operation may be crucial for the success of an investigation of cases of dissemination of terrorist propaganda or terrorist expertise.

Law enforcement authorities should also be in a position to ask hosting providers based in the European Union to disable access to relevant websites, within the limits set out in the Directive on electronic commerce and according to national provisions implementing this instrument. However, this is only a desirable objective in those cases where disabling access to a relevant website does not interfere nor conflict with monitoring and investigation purposes..

Furthermore, in the long term, and from a general perspective, the messages disseminating terrorist propaganda and terrorist expertise through the Internet would be included in the global strategy of the EU to fight illegal content, including the dialogue and co-operation with third countries which, knowingly or not, are harbouring terrorism-related websites.

2. Enhancing the capacities and expertise of law enforcement authorities to counter the dissemination of terrorist propaganda and terrorist expertise, especially through the Internet.

Law enforcement authorities should be conveniently trained, sufficiently equipped and supported by experts both on languages and IT, in order to detect and analyse violent radical content on the Internet. Pro-active policing of such content on the Internet may provide for

key information in order to understand terrorist trends, anticipate terrorist actions and prevent attacks. Efficient detection and analysis may also provide for crucial data contributing to successful investigations and prosecutions. In this sense, law enforcement authorities should be equally trained, equipped and supported to trace and identify the individuals behind the dissemination of terrorist propaganda and terrorist expertise. They should be able to request traffic and location data from telecommunication operators within the limits set out by the Directive on data retention and in accordance with the national provisions implementing this instrument.

The importance of the data that may be obtained through monitoring and analysis of violent radical content on the Internet, either as pro-active policing or deriving from the investigation of a specific case, makes the disablement of access to websites a secondary objective. As explained above, disabling access to a relevant website is only a desirable objective when it does not interfere or conflict with monitoring or investigating purposes.

Such interference or conflict should be considered on a case by case basis. The decision implies weighing the benefits from closing down a website in terms of prevention of radicalisation and avoiding the risk of availability of certain information (i.e. the vulnerabilities of eventual targets of terrorist attacks) and the drawbacks of both giving up an information channel and alerting the terrorist activists and supporters behind the relevant contents.

4. SECTION 4: POLICY OPTIONS

4.1. Option 1: No policy change

This option implies that no new legislative or other measures will be adopted, neither aiming at adopting a new instrument nor amending an existing one. However, in the no policy change scenario, it is necessary to take into consideration the Council of Europe Convention on the prevention of terrorism of 2005, which recently entered into force. Under this instrument, parties must adopt the necessary measures to establish public provocation to commit a terrorist offence, recruitment for terrorism and training for terrorism, when committed unlawful and intentionally, as criminal offences under their domestic law, irrespective of the actual commission of a terrorist offence. Therefore, the Council of Europe Convention on the prevention of terrorism provides for a harmonised legal basis to fight the use of the Internet as a means for public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism including through the Internet, overcoming the obstacles identified in the relevant provisions of the Framework Decision to cover these forms of behaviour. It will lead to the harmonisation of Member States' legislation provided that all of them sign and ratify the Convention. It follows that, even if no measure is taken at EU level, a co-ordinated response to the dissemination of terrorist propaganda and terrorist expertise by Member States would be possible.

In particular, the relevant provisions, Articles 5 to 8 of the Convention, read as follows:

"Article 5 – Public provocation to commit a terrorist offence

1. For the purposes of this Convention, "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such

conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.

2. Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

Article 6 – Recruitment for terrorism

1. For the purposes of this Convention, "recruitment for terrorism" means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group.

2. Each Party shall adopt such measures as may be necessary to establish recruitment for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

Article 7 – Training for terrorism

1. For the purposes of this Convention, "training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence, knowing that the skills provided are intended to be used for this purpose.

2. Each Party shall adopt such measures as may be necessary to establish training for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

Article 8 – Irrelevance of the commission of a terrorist offence

For an act to constitute an offence as set forth in Articles 5 to 7 of this Convention, it shall not be necessary that a terrorist offence be actually committed."

Although these provisions do not explicitly refer to the commission of such offences via the Internet, they are in fact applicable irrespective of whether they are committed over the internet or not, as the explanatory report to the Convention clarifies. These provisions therefore cover the issues of dissemination of terrorist propaganda aiming at mobilisation, recruitment or fund-rising as well terrorism expertise through the Internet.

Moreover, Article 9 (2) of the Convention clarifies that attempting to recruit or train must also be made punishable. Finally, recruitment is widely defined: soliciting another person to commit or participate in the commission of a terrorist offence constitutes recruitment even if the person is not asked to join a group or association.

4.2. Option 2: Forbidding internet services providers to give access to material aiming at public provocation to commit terrorist offences, recruitment or training for terrorism

This option implies the introduction of a new legislative instrument specifically addressed to internet service providers or the amendment of the existing provisions. It intends that internet service providers based in Europe apply systematically blocking techniques in order to prevent internet users from accessing material aiming at public provocation to commit terrorist offences, recruitment or training for terrorism. This material should be kept outside EU cyber-space.

Existent technical methods to implement such obligation include dynamic filtering or black lists systems based on IP, DNS or URL filtering.

Dynamic filtering: "this is a system in which software examines incoming Internet content and determines whether to permit the Internet user access the content based on how closely that content conforms to a set of censorship criteria"[54].

Black lists systems: these are systems in which Internet users are impeded access to prohibited websites contained in a black-list, previously created by individuals, through different technical solutions:

(a) IP filtering or packet dropping systems: "they are conceptually very simple. Packets destined for the IP addresses of the websites to be blocked are discarded and hence no connection can be made to the servers. The main problem with packet dropping is the collateral damage that it causes because all of the web content on the particular IP address will become inaccessible. This can be very significant"[55].

(b) DNS filtering or DNS poisoning systems: "they work by arranging that DNS lookups for the hostnames of blocked sites will fail to return the correct IP address. This solution also suffers from overblocking in that no content within the blocked domain remains available. However, the over-blocking differs from that of IP filtering in that it does not extend to blocking other domains that are hosted on the same machine. There is also some "under-blocking" in that a URL containing an IP address, rather than a hostname, would not be affected; because a browser would simply use the IP address and would not consult the DNS at all"[56].

(c) URL filtering or content filtering systems: "they will not only block entire websites but can also be used to block very specific items, such as a particular web page or even a single image. They determine that the URL being accessed is one of those to be blocked and then ensure that the corresponding content is not made available. This type of system is extremely accurate in blocking

---

54 See "Countering Militant Islamist radicalisation on the Internet: a user driven strategy to recover the web", Institute of European Affairs 2007, referred to above, in footnote 6, p. 91.

55 See "Failures in a Hybrid Content Blocking System", by Richard Clayton, http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf

56 See "Failures in a Hybrid Content Blocking System", by Richard Clayton, mentioned above, footnote 70.

exactly what is on the list of URLs, no more, no less, and hence there should be no overblocking (provided, of course, that the list of URLs was correct in the first place). Quite clearly, web proxies are ineffective at blocking content if their usage is optional. Hence it must be arranged that all customer traffic passes through the proxy, leading to a considerable expense in providing equipment that can handle the load. Also, to prevent a single point of failure, the equipment must be replicated, which considerably increases the cost. The bottom line for most ISPs considering blocking systems is that although content filtering is the most precise method, it is also far more expensive than the alternatives"[57].

Encouraging blocking through the industry's self-regulation or through agreements with industry, without the previous adoption of legal measures outlawing the dissemination of terrorist propaganda and terrorist expertise has been ruled out. The adoption of blocking measures necessarily implies a restriction of human rights, in particular the freedom of expression and therefore, it can only be imposed by law, subject to the principle of proportionality, with respect to the legitimate aims pursued and to their necessity in a democratic society, excluding any form of arbitrariness or discriminatory or racist treatment. This is also the approach of the Communication on cyber-crime which foresees the development of EU-level voluntary agreements and conventions between public authorities and private operators as regards illegal content, but not harmful content.

Adopting legal measures obliging internet service providers to remove or disable access to the dissemination of terrorist propaganda or terrorist expertise they host has also been ruled out. As explained under Section 2.1.3 b, the issue of the speedy re-apparition of websites that have been closed down must be considered: when a website is successfully removed from a host server, it reappears very easily under another name. It can also reappear outside the jurisdiction of the European Union, in order to avoid the eventuality of being closed down once more. Therefore, the removal or disablement of access to terrorist propaganda or terrorist expertise by internet service providers hosting such information, without the possibility to open an investigation and prosecute the one responsible behind such content, appears inefficient.

4.3. Option 3: Enhancing law enforcement authorities' capacities and expertise to counter the use of the Internet for terrorist purposes

This option does not require the adoption of a legislative instrument but the Commission's financial support, which should be foreseen in the annual work programmes implementing the Council Decision of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme Prevention of and Fight against Crime.

The Commission's support could include the co-financing of different projects aiming at:

- stimulating the co-operation between academic experts and law enforcement authorities to provide these with the expertise they lack;

---

57 See "Failures in a Hybrid Content Blocking System", by Richard Clayton, mentioned above, footnote 70.

- enhancing co-operation between Member States to develop and exchange efficient methods of monitoring the internet for radical violent content, and
- strengthening specific training required for law enforcement authorities and others involving in countering the terrorist use of the internet.

It could also include the contract of studies on:

- non-legislative measures to prevent the distribution of violent radical content on the Internet, including notice and take down procedures and co-operation between NGOs and law enforcement authorities, and
- methodologies and adapted technological tools to efficiently detect violent radical content on the Internet .

Option 3 would in this manner provide for practical measures to support law enforcement authorities in the acquisition of further capacities and expertise to counter more efficiently the use of the Internet for terrorist purposes.

Options 4 and 5: Ensuring that Member States explicitly incriminate the use of the Internet as a means of public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism

Both options would ensure that Member States explicitly incriminate the use of the Internet as a means of public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism.

4.4. Option 4: Urging Member States to sign and/or ratify the Council of Europe Convention on the prevention of terrorism.

In this case, a political statement should be made urging Member States to sign and/or ratify the Council of Europe Convention on the prevention of terrorism. The incrimination of public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism would not become EU law. Harmonisation would however be achieved through the signature and ratification of the Convention.

It must be clarified that, under Articles 24 and 38 TEU, the European Union could have acceded to the Convention if the Presidency, authorised by the Council and assisted by the Commission, had negotiated on behalf of all Member States. However, this did not occur in the case of the Council of Europe Convention on the prevention of terrorism, and therefore, the EU cannot presently sign and ratify the Convention - this can only be done by the Member States individually.

4.5. Option 5: Revising the Framework Decision on combating terrorism in order to introduce parallel offences to those foreseen under the Council of Europe Convention

This option implies the introduction of an EU legislative instrument or the amendment of an already existing one. Given the existence of the Framework Decision on combating terrorism that already contains terrorist offences, offences related to terrorist groups and terrorist-linked offences, it is preferable to amend this instrument rather than to introduce a new one. As for

the content of the amendment, it seems appropriate to opt for the level of incrimination of the Council of Europe Convention of the prevention of terrorism. This reasoning also applies to the formulation of the new offences. As explained above, the Convention tackles the new modus operandi of terrorist, including the use of the Internet as a means for public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism. It therefore overcomes the obstacles to cover the dissemination of terrorist propaganda and terrorist expertise identified in the Framework Decision on combating terrorism. Additionally, the Convention was elaborated bearing in mind the relevant case-law of the European Court of Human Rights, so that human rights and especially the freedom of expression are duly taken into account. Finally, it is advantageous to both the European Union and the Council of Europe as institutions, but also particularly for their Member States, if there is a consistency in approach between the two organisations. This sends a clear political message that the two organisations work in the same direction. At a more practical level, it should be avoided that Member States would need to implement in their national legislation two different international legal instruments. This is especially important considering the fact that in many Member States of the European Union ratification procedures related to the Council of Europe Convention are currently underway.

Despite the existence of the Council of Europe Convention on the prevention of terrorism, a revision of the Framework Decision on combating terrorism so that it would also cover these forms of behaviour would not amount to a mere formal change. It would entail significant differences in terms of the application of harmonised rules on penalties and jurisdiction and ensure the application of related EU instruments.

5. SECTION 5: IMPACTS

The impact of particular policy options on specific issues is measured below as a function of the magnitude of the impact. The magnitude of each impact should be viewed as the level of influence a particular policy option would have on specific issues falling within the security, economic and human rights context.

Table of symbols (distinguishes "-" for costs and "+" for benefits

Small magnitude	- / +
Medium magnitude	-- / ++
Significant magnitude	- - - / +++
No impact	0

5.1.1 Option 1: No policy change

As a preliminary clarification, it must be taken into account that the existence of the Council of Europe Convention on the prevention of terrorism considerably mitigates or modifies the impacts of non action at EU level. Had the Convention not existed, the effects resulting from no policy change would have greatly differed from those exposed below.

5.1.2. Security impact

As explained under section 1, all other things being equal, the fast growing number of users will make the Internet in the future even more important in modern society than it is today. Therefore, the importance of online terrorism could only be expected to increase and, with it, the role of the Internet as a key instrument to fuel violent radicalisation and facilitate terrorist attacks. Terrorist propaganda and terrorist expertise would reach an even larger audience which would easily access messages providing for encouragement, justifications and expertise to perform a terrorist attack. The number of both supporters and activists within the territory of the European Union is in consequence expected to rise.

Helped by the Internet, terrorists would become even more de-centralised, faster and more difficult to trace. Law enforcement authorities would lack the appropriate legal instruments to combat the new modus operandi of terrorists, who would exploit this security gap to their advantage. Lack of legal basis or lack of harmonisation of national legislation and consequently deficient international cooperation regarding the use of the Internet for terrorist purposes would substantially hinder law enforcement authorities in their task of fighting terrorism.

This worst case scenario will not however become true because the Council of Europe Convention on the prevention of terrorism provides for a harmonised legal basis to fight the use of the Internet as a means for public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism. The harmonisation of Member States' legislation would therefore be achieved if all of them sign and ratify the Convention, which is an outcome that cannot be guaranteed. Although such harmonisation will not bring about the same results as legislation at EU level[58], it would certainly achieve some positive results and contribute to counter the present successful spread of violent radicalisation through the Internet.

In particular, those disseminating terrorist propaganda and terrorist expertise would be held liable for public provocation to commit a terrorist offence, recruitment or training for terrorism throughout the EU. In addition, the incrimination of such behaviour in all Member States, would amount to an increased co-operation of national law enforcement authorities both with industry and law enforcement authorities in other Member States in the context of criminal investigations. In particular, the use of the co-operation mechanisms foreseen under the Directive on electronic commerce and the data retention Directive would be possible concerning the dissemination of terrorist propaganda and terrorist expertise in all Member States. Law enforcement authorities could request traffic and location data in the context of the investigation of public provocation to commit a terrorist offence, recruitment or training for terrorism as well as the disablement of access to terrorist propaganda or terrorist expertise according to the national rules implementing, respectively, the Directive on data retention and the Directive on electronic commerce It should be stressed that the regime set out under both instruments remains unchanged. In particular, the liability regime foreseen under the Directive on electronic commerce is fully respected.

The security impact of this instrument is mitigated by the existence or current elaboration of provisions dealing with the dissemination of terrorist propaganda in seventeen out of the

---

58 See the added value of the revision of the Framework Decision in relation to the existing Council of Europe Convention on the prevention of terrorism. above, in section 4, option 5.

eighteen Member States that answered the respective questionnaire (see Annex I). In addition, provisions dealing with terrorist expertise are applicable in nine of those Member States. Concerning the Member States' legislation applicable to terrorist propaganda, it is important to stress that the scope of existing national provisions is usually narrower than public provocation to commit a terrorist offence and recruitment for terrorism. In particular, while direct provocation may be considered punishable in all those Member States that have legal measures in place, indirect provocation, explicitly punishable under the Council of Europe Convention, is not covered in many cases. This is a very important issue since the inclusion of indirect provocation in the Convention constitutes a key step forward. It represents the results of an ad hoc committee of the Council of Europe ("CODEXTER-apologie") and is in line with existing case law of the ECHR[59]. This case law provides for some examples of cases where indirect provocation (defending the ideology or supporting the views of a terrorist) were not considered to be covered by the right to freedom of speech[60]. There is, therefore, a security gap which the Convention can address.

- Magnitude of the impact on security: +

5.1.3. Economic impact:

Indirect economic impact on public authorities and tax-payers:

There are no direct costs identified. However, the ratification of the Convention on the prevention of terrorism by Member States might involve indirect costs. The new harmonised legislation to combat the terrorist threat would amount to an increased co-operation of national law enforcement authorities both with industry and law enforcement authorities in other Member States in the context of criminal investigations. This should lead to improved results, which implies more successful investigations and more prosecutions than presently. However, further cross-border co-operation and increased contacts with industry as well as increased prosecutions involve an additional work-load.

The hypothesis of an additional work-load resulting from the signature and ratification of the Council of Europe Convention of the prevention of terrorism by Member States is in line with Europol's report TE-SAT 2007. The report states that the number of police investigations into terrorist propaganda seems small compared with the amount of material circulating on the Internet adding that this is partially explained by the lack of legal basis for arrests or investigations using the Internet in this manner[61].

If the increased activity of law enforcement authorities required the allocation of further resources, tax-payers would not necessarily assume higher taxes: the budget allocated to law enforcement and security may be increased at the expense of other State's policies.

- Magnitude of the impact on economy: -

Indirect economic impact for companies and consumers:

---

59 See explanatory report to the Council of Europe Convention on the prevention of terrorism, mentioned above, footnote 13.

60 See section 5.1.3, impact on human rights of option 1.

61 See the EU Terrorism Situation and Trend Report 2007 of Europol, p. 21.

No direct economic impact derives from the absence of legal measures at EU level. However, the Council of Europe Convention on the prevention of terrorism may indirectly lead to an increased use of the co-operation mechanisms foreseen under the Directive on electronic commerce and the data retention Directive. Further requests of removing material or providing information by law enforcement authorities can easily result in additional work-load for internet service providers.

It must be clarified, however, that the signature and ratification of the Convention on the prevention of terrorism by all Member States would not create or impose any new co-operation channel. Both the Directive on electronic commerce and the data retention directive have already foreseen such collaboration. The inclusion of new offences under national law would simply lead to an increased use of existing mechanisms of co-operation. But even if no new co-operation channels are created, a rise in the number of investigations related to the new offences would logically imply an additional work-load for internet service providers. These would have to assume the resulting costs unless they were able to transfer them to consumers or national authorities without seeing their sales figures reduced.

In particular, internet service providers are especially concerned with the costs deriving from the co-operation mechanisms foreseen in the Data retention Directive. Data retention involves the obligation of collection, storage and retrieval of certain traffic data. While internet service providers must automatically collect and store the relevant data, retrieving only takes place in case the data are requested by law enforcement authorities. The revision of the Framework Decision on combating terrorism would therefore not imply any change to the collection and storage of data. It would only affect the retrieval of data, in all likelihood increasing the number of requests to internet service providers.

When the Data Retention Directive was under preparation, EuroISPA indicated that costs associated with data retrieval would be very high, taking into account increased levels of data retention for extended periods[62].

However, the development, maintenance and staffing of data retrieval systems is already required by the data retention Directive, and the option contemplated here would not change that. More numerous retrieval requests under the new offences of public provocation, recruitment and training would therefore simply imply further use of existing infrastructure. Expected additional costs for internet service providers will with all probability be limited to an increased work-load of staff assigned to these tasks. The work-load of attending to such request is estimated at a maximum of four hours per request. This must be related to the number of arrests of terrorist suspects in 2006 in the European Union (706) as well as the number of internet service providers. In 1998, the estimations were that there were around 3,000 internet service providers in Western Europe alone. It should be assumed that many arrests do not require requesting traffic or location data from providers and that some data can lead to the arrest of more than one individual but also that some information obtained from providers does not lead to any arrest. Under the assumption that there are currently at least 5,000 providers in the EU, the number of hours of work per year and internet service provider that could be originated with the introduction of the three new offences which already exist in some Member States, is not considerable.

---

62 Answer of EuroIspa to DG INFSO – DG JAI Consultation Document on Traffic Data Retention, 15 September 2004, http://www.euroispa.org/23.htm.

As regards removing or disabling access to certain websites under the Directive on electronic commerce, the same estimation – a maximum of four hours work per request - can be made, including the notification to the website owner. Once again, the number of terrorist arrests and the estimated number of internet service providers in the EU greatly reduces the impact of this measure per individual service provider. Although the number of websites disseminating terrorist propaganda and terrorist expertise is relatively high, only a limited portion of these are said to be hosted by internet service providers based in the EU[63]. Most importantly, most investigations do not seek to close down the websites but to monitor them, since very valuable information may be obtained[64].

It should be kept in mind that, insofar as the impact on security of option 1 is mitigated by existing legislation in Member States, the economic impact is also reduced. The number of Member States already providing for some legal measures mentioned above should be taken into consideration as indicators of the minimal estimated additional costs.

- Magnitude of the impact on economy: -

---

[63] See the newsletter of the Department of Justice of the US attorney's office Northern District of Indiana, of 28.7.2004, http://www.iwar.org.uk/news-archive/anti-terrorism-advisory-council/atac-vol-07-04.pdf, which states that the US hosts 76 percent of Islamist terrorist websites.

[64] The coordinated monitoring of websites run by terrorist activists and supporters is the aim of the German initiative Check the Web, that was launched in 2006 and has achieved the establishment of a portal in Europol serving as a data base for this kind of sites and avoiding double working – concerning all detection, translation and monitoring.

5.1.4. Human rights impact:

Direct impact on freedom of expression

The new offences introduced by the Convention on the prevention of terrorism imply a direct impact on the right to freedom of speech, especially the offence of public provocation to commit terrorist offences. Nevertheless, the explanatory report to the Convention clarifies that the Convention on the prevention of terrorism contains several provisions concerning the protection of human rights and fundamental freedoms, both in respect of internal and international co-operation on the one hand and as an integral part of the new criminalisation provisions (in the form of conditions and safeguards). Articles 12, "conditions and safeguards" and 21 "discrimination clause" of the Convention are particularly important in this respect. Namely, Article 12 (1) contains an explicit obligation of the Member States to ensure that the establishment, implementation and application of the criminalisation for which it provides are carried out while respecting human rights obligation, in particular the right to freedom of expression, freedom of association and freedom of religion. It further specifies that the establishment, implementation and application of the offences shall furthermore be subject to the principle of proportionality, with respect to the legitimate aims pursued and to their necessity in a democratic society while excluding any form of arbitrariness or discriminatory or racist treatment. The protection of human rights and fundamental freedoms, continues the explanatory report, is a crucial aspect of the Convention, given that it deals with issues which are on the border between the legitimate exercise of freedoms, such as freedom of expression, association or religion, and criminal behaviour.

Concerning public provocation to commit terrorist offences, it is indirect provocation which raises more concerns[65]. However, paragraphs 86-105 of the explanatory report to the Convention clearly stress the human rights compliant approach followed by the Council of Europe in drafting the provision in question. These paragraphs recall that freedom of expression is one of the essential foundations of a democratic society and applies, according to the case-law of the European Court of Human Rights, not only to ideas and information that are favourably received or regarded as inoffensive but also to those that "offend, shock or disturb". Nevertheless, it is noted that, in contrast to certain fundamental rights which are absolute rights and therefore admit no restrictions, such as the prohibition of torture and inhuman and degrading treatment or punishment, interference with, or restrictions on freedom of expression may be allowed in highly specific circumstances. Article 10, paragraph 2 of the ECHR lays down the conditions under which restrictions on, or interference with, the exercise of freedom of expression are admissible under the ECHR[66], while Article 15 of the ECHR provides for possible derogations in time of emergency. The explanatory report gives the

---

65 See, in particular, paragraph 97 of the Explanatory report to the Council of Europe Convention on prevention of terrorism: "Direct provocation does not raise any particular problems in so far as it is already a criminal offence, in one form or another, in most legal systems. The aim of making indirect provocation a criminal offence is to remedy the existing lacunae in international law or action by adding provisions in this area".

66 Article 10(2) of the ECHR states: "The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary".

example of incitement to racial hatred that cannot be considered admissible on the grounds of the right to freedom of expression[67]. The same goes, it clarifies, for incitement to violent terrorist offences and explains that the Court of Human Rights has already held that certain restrictions on messages that might constitute an indirect incitement to violent terrorist offences are in keeping with the ECHR.

Furthermore, the UN Special Rapporteur on the protection of human rights and fundamental freedoms while countering terrorism highlighted the human rights compliant approach of the Convention, stating that the Council of Europe Convention on the Prevention of Terrorism, which includes a provision calling on states to criminalize public provocation to commit a terrorist offence, is "a sound response which would respect human rights". The Special Rapporteur viewed favourably the Convention’s definition of "public provocation" since it was based on a "double requirement of a subjective intent to incite (encourage) the commission of terrorist offences and an objective danger that one or more such offences would be committed"[68].

Therefore, it can be concluded that the restrictions on freedom of speech and access to information included in the Council of Europe Convention are in fact compliant with international human rights norms. The restrictions imposed by the new offence of public provocation to commit terrorist offences are covered by Article 10(2) of the ECHR.

The European Court of Human Rights provides for very interesting examples of cases where it was found that interferences with freedom of expression in connection with the fight against terrorism complied with Article 10 of the ECHR[69]. Furthermore, as explained above, such case-law was taken into consideration for the introduction of the new offences, especially the public provocation to commit a terrorist offence.

In the case Brind and others v. UK, for example, the British Government ordered the applicants, a television producer and five other broadcast journalists, to refrain at all times from sending any broadcast matter which consisted of or included statements expressing or supporting the views of several terrorist groups. The European Commission of Human Rights found, in the circumstances of the case and bearing in mind the margin of appreciation permitted to States and the importance of measures to combat terrorism, that it could not be said that this interference with the applicants' freedom of expression was disproportionate to the aim sought to be pursued. Consequently the application was manifestly ill-founded and therefore inadmissible.

In the case Hogefeld v. Germany, the applicant was a former member of the Red Army Fraction (RAF), a left-wing extremist terrorist movement that had been responsible for numerous attacks on high-ranking personalities in Germany since the early seventies. In 1993, the applicant was arrested and detained on remand. Subsequently, German courts denied the request of a radio journalist to allow an interview with the applicant because such an interview would conflict with the purpose of the detention on remand, since it was to be

---

67 See Article 9, paragraph 2, of the Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965.

68 See paragraph 57 of the Report of the Counter-Terrorism Committee to the Security Council on the implementation of Resolution 1624 (2005) (document S/2006/737 of 15 September 2006).

69 See Collection of relevant case-law of the European Court of Human Rights related to "apologie du terrorisme" and "incitement to terrorism", Council of Europe, CODEXTER (2004) 19.

expected, in respect of the declaration made by the applicant during the trial, that the applicant would explain and advocate ideological positions of the RAF, which would amount to a new act of participation in a terrorist organisation. The European Court of Human Rigths noted that in assessing this limitation of the freedom of expression the applicant's personal history had to be considered. As the applicant was most probably one of the main representatives of an organisation which had waged a murderous war against the public order of the Federal Republic of Germany for more than twenty years, the words of the applicant could possibly be understood by supporters as an appeal to continue the activities of the RAF, even if they did not directly incite violence. In consequence, it was concluded that there had been no breach of Article 10 of the ECHR.

These two cases clearly show restrictions of freedom of expression stemming from the incrimination of public provocation to commit a terrorist offence, and how they nevertheless comply with Article 10 of the ECHR. In two other cases the European Court of Human Rights found, on the contrary, that Article 10 of the ECHR had not been respected[70]. These judgements help to understand which restrictions of human rights would not be acceptable in relation with the offence of public provocation to commit a terrorist offence.

In Sener v. Turkey, charges were brought under the Prevention of Terrorism Act against an author of an article containing separatist propaganda. It was concluded that the subsequent conviction constituted a violation of Article 10 of the ECHR because the article taken as a whole did not glorify violence. Nor did it incite people to hatred, revenge, recrimination or armed resistance.

Another relevant case is Castells v. Spain. Mr. Castells, a senator elected on the list of Herri Batasuna, a political movement seeking the independence of the Basque Country[71], was convicted for having written an article published in a weekly magazine which contained insults directed against the Spanish nation and its institutions. In the trial, he was denied the opportunity to prove the truth of his allegations and his good faith, because it was held that, lacking precision, it was impossible to demonstrate their truth. The European Court of Human Rights attached decisive importance to the fact that Mr. Castells was a political representative of the opposition party, criticising the Government, and to the alleged inadmissibility of evidence on behalf of the applicant, and ruled that in sum there had been a violation of Article 10 of the ECHR.

- Magnitude of the impact on freedom of expression : -

It should be clarified that the Convention does not imply an impact on the right to privacy and data protection. Existing rules on the right to privacy and data protection at both EU and national level remain unchanged. It is true that law enforcement authorities may request traffic and location data from internet service providers in order to trace terrorist activists and supporters behind the dissemination of terrorist propaganda and terrorist expertise. However, these requests will have to be submitted and dealt with under the regime established in the existing Directive on data retention and in accordance with the national rules implementing

70 See Collection of relevant case-law of the European Court of Human Rights related to "apologie du terrorism" and "incitement to terrorism", mentioned above, footnote 87.

71 It should be noted that the decision of the ECHR dates from 24 April 1992. Herri Batasuna was declared illegal on 27 March 2003 by the Spanish Supreme Court for its support to the terrorist group ETA.

this instrument. Therefore, the signature and ratification of the Convention does not entail any modification of such regime nor, therefore, an impact on the right to privacy and data protection.

Indirect impact on right to life and to integrity

Moreover, the explanatory report of the Convention also states that the human rights that must be respected are not only the rights of those accused or convicted of terrorist offences, but also the rights of the victims, or potential victims, of those offences. The incrimination of public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism has as final aim the protection of human rights of potential victims, in particular the right to life and the right to physical and mental integrity. In fact, such protection concerns all citizens, since experience shows that anyone is a potential victim. From this point of view, the Convention has a positive, although indirect impact on human rights that should also be taken into consideration. The magnitude of such impact logically corresponds to the level of increased security achieved by the Convention.

- Magnitude of the impact on right to life and to integrity: +

5.2. Option 2: Forbidding internet service providers to give access to material aiming at public provocation to commit terrorist offences, recruitment or training for terrorism

5.2.1. Security impact

Option 2 aims at keeping messages provoking people to commit terrorist offences, recruiting for terrorism and training for terrorism outside EU cyberspace. It should be clarified however that impeding completely that a certain kind of content is accessible to the public through the Internet is technically unfeasible. Existing technical methods of filtering (dynamic filtering or black lists systems based on IP, DNS or URL filtering) do not constitute a perfectly solid barrier.

First of all, existing methods of filtering can be circumvented[72]. Moreover, such systems have been designed specifically for web access. They do not function appropriately for most other Internet services and cannot be applied to “peer-to-peer” technologies. Information-sharing using encryption tools, for example, cannot be blocked or usefully intercepted by internet service providers[73].

In addition to these weaknesses, methods based on a black list suffer from the inevitable incompleteness of the list. Given the volume of the material circulating through the Internet, as well as the speedy edition of new material and re-edition of material in new websites, a black list is bound to be seriously incomplete and out-dated. Therefore, the efficiency of filtering is limited by the incompleteness of the black-list in the first place.

But dynamic blocking also presents initial imperfections. "It is based on an automated form of censorship, bypassing a black list created by humans and using instead a set of criteria of characteristics of the kind of material that should be censored"[74]. Pre-fixed criteria will not be able to cover all cases of contents that should be blocked. There will necessarily be some materials that do not meet the set of criteria and still aim at provoking to commit terrorist offences, recruitment for terrorism or training for terrorism.

In consequence, if filtering methods were to be applied, terrorist propaganda and terrorist expertise would still be accessible from the European Union for those seeking for the prohibited contents and having some Internet literacy. The dissemination of such content would only be hindered but not eliminated. It is questionable whether such additional difficulties would be a true deterrent for those determined to access violent radical contents or

---

72 Authors do not agree on the ease of the circumvention and while some argue that filtering methods are easily circumvented, others state that most circumvention techniques are technically complex or burdensome to the user or need the cooperation of a third party. See "Government mandated blocking of foreign Web content", by Maximillian Dornseif, http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf. However, all seem to agree on the feasibility of circumventing filtering methods. In this sense, Klaus Langefeld, technical expert of EuroIspa, states that "blocking or removing anything but the source is an illusion and will not be effective". See "Investigating Internet traffic", p. 16, http://www.euroispa.org/23.htm.

73 Response of EuroISPA, the European Association of internet service providers to the second questionnaire issued by the Commission in view of the elaboration of the impact assessment on the revision of the Framework Decision on combating terrorism.

74 See "Countering Militant Islamist radicalisation on the Internet: a user driven strategy to recover the web", Institute of European Affairs 2007, referred to above, in footnote 6, p. 91.

would only prevent the access of those that would come across the material accidentally or consult it out of curiosity. Furthermore, it should be considered that the access of one individual is enough to record audio or video files or copy documents containing terrorist propaganda or terrorist expertise that may be later easily distributed through mailing lists or other electronic means.

In conclusion, the role of the Internet as a means to fuel violent radicalisation and facilitate terrorist attacks would not disappear. In addition, as explained above, authors of messages aiming at provoking others to commit terrorist offences, recruiting for terrorism and training for terrorism could not be prosecuted. This represents an important weakness from the point of view of security.

- Magnitude of the impact on security: +

5.2.2. Economic impact

Indirect economic impact on public authorities and tax-payers:

It would be similar to the one described above under option 1.

Direct economic impact on internet service providers and consumers

In this case, there would be a direct economic impact on internet service providers, deriving from the costs of filtering technology. The level of costs differs, however, from one method to another. "Filtering access to specific IPs is comparatively cheap because the "router" machines that internet service providers use to provide access to the Internet to their customers have built-in blocking capabilities. Unlike other web filtering technologies, no further equipment is necessary"[75]. By contrast, URL filtering would be extremely expensive: "comparing all URLs flowing through an internet service provider's network with a list of URLs to be blocked is "expensive" in the computational sense – it requires a significant amount of computing power. Performing these computations would slow down the switches (the hardware that bridges different parts of computer networks together) and routers substantially, decreasing the overall capacity of the network and degrading the speed of Internet access provided to customers. Internet service providers would be required to purchase additional switches and routers to maintain the network’s prior level of traffic"[76]. Costs resulting from DNS and dynamic filtering would be in between. The former "can also be difficult for some Internet service providers to manage, depending on the configuration of their systems"[77]. In the case of the later, "internet service providers may have to purchase additional hardware to allow for the computationally expensive inspection of incoming traffic by the filtering software, although some internet service providers already offer this service as an option to their clients"[78].

---

75 See "Countering Militant Islamist radicalisation on the Internet: a user driven strategy to recover the web", Institute of European Affairs 2007, referred to above, in footnote 6, p. 89.

76 See "Countering Militant Islamist radicalisation on the Internet: a user driven strategy to recover the web", Institute of European Affairs 2007, referred to above, in footnote 6, p. 92.

77 See "Countering Militant Islamist radicalisation on the Internet: a user driven strategy to recover the web", Institute of European Affairs 2007, referred to above, in footnote 6, p. 90.

78 See "Countering Militant Islamist radicalisation on the Internet: a user driven strategy to recover the web", Institute of European Affairs 2007, referred to above, in footnote 6, p. 91.

Internet service providers would suffer an economic impact unless they are able to transfer the total of the incurred costs to consumers without seeing their sales figures reduced.

Indirect impact on internet service providers and consumers

In addition to the costs mentioned before, incorrect blocking of legitimate material represents an economic impact. Collateral blocking may have serious legal and economic implications. Blocking users from accessing commercial websites may cause important losses to the companies selling or providing services through the Internet as well as to their clients. Furthermore, consequences of interrupting the advertising which finances most websites must be taken into account. Therefore, although in terms of initial investment it is considered a relatively cheap system, IP filtering might end up being the most expensive. Although not to the extreme of IP filtering, DNS poisoning is also prone to over-blocking. URL filtering, which is so expensive in terms of initial investment, is by contrast much more precise and less likely to cause collateral blocking. In this sense, URL filtering may end up being not such an expensive system. As for dynamic blocking, since it automates censorship, bypassing a black list created by humans and using instead a set of criteria of characteristics of the kind of material that should be censored, there is an obvious risk that legitimate contents fulfil the predetermined criteria and are consequently blocked.

It should be noted that the most of the direct costs of URL filtering and indirect costs of IP filtering referred to above can be overcome by URL hybrid filtering. This method combines the best of both IP and URL techniques: it is considered as precise as pure URL filtering and yet considerably cheaper, because filtering based on URL is only applied to pre-selection of websites based on IP filtering.

The economic costs analysed so far may be summarized as follows:

Economic costs for ISPs	Direct costs	Indirect costs	Global assessment of costs
IP filtering	-	---	--
URL filtering	---	0	--
URL hybrid filtering	-	0	-
DNS filtering	--	--	--
Dynamic filtering	--	-	-/--

The costs deriving from imposing any of these filtering methods to all internet service providers based in the EU is impossible to calculate. EuroISPA, the world's largest association of Internet Service Providers, representing approximately 1,000 internet service providers across the EU, considers it unfeasible to provide for any figure, arguing that there are so many variables in the composition of systems that might be used for blocking, that it is

not possible to give general figures. Johnny Ryan[79] confirms this statement detailing the factors that make a general estimation of costs impossible, in particular:

1. The different sizes of networks operated by internet service providers and the amount of traffic passing across it. This is a very important variable in the implementation of a filtering method. It determines how much additional hardware or personnel will be required to process the filtering without reducing the speed of the network.

2. The network typology that changes from one internet service provider to another. The more centralised the network, the fewer the locations where the filtering must be implemented and the less expensive it becomes, since equipment and personnel costs depend on the number of places where the filtering is carried out.

3. The wide spectrum of technology with different capabilities used by the different internet service providers so that they would not be in the same position if they were obliged to implement a filter method. Some internet service providers would be ready to filter but others would have to buy new expensive hardware.

If general costs are impossible to estimate, the costs of a specific method of filtering implemented by a single internet service provider can be calculated, but must be considered a specific example only. HEA Net is an Irish research and education network which provides broadband internet access to approximately 100,000 computers at 4,000 schools and has implemented URL filtering. The costs of developing and building this system from scratch have been close to 1,000,000 euros, which represents around 10 euros per computer. This case-study represents an indicator of the upper-limit of what the most expensive method of filtering – URL-filtering - might cost, if the internet service provider had to start from zero. It does not however include maintenance costs[80].

Additional direct economic impact deriving from filtering methods relying on a black list

"A system based on IP, DNS or URL filtering relies on a black-list of prohibited websites. If a black-list was introduced to censor violent radicalisation material in the EU, a centrally maintained and up-dated black list could be instantaneously accessed by ISPs operating throughout the Union, instantly blocking newly added websites"[81]. Therefore, for these filtering methods, it is necessary to study the costs deriving from maintaining a black-list, although it should be noted that centralisation would moderate the costs considerably.

Furthermore, these costs should not necessarily be supported by internet service providers or at least not entirely, since law enforcement should be involved in the selection of the list's elements. Actually, if all costs were assumed by public authorities, taking into consideration the ongoing work in many Member States to identify and study this kind of material on the Internet, a central black-list might actually become economically efficient, by avoiding double

---

79 "Countering militant Islamist radicalisation on the Internet – A user driven strategy to recover the web", mentioned above, in footnote 6, pp. 108-109.

80 See "Countering Militant Islamist radicalisation on the Internet: a user driven strategy to recover the web", Institute of European Affairs 2007, referred to above, in footnote 6, pp. 110-112.

81 See "Countering Militant Islamist radicalisation on the Internet: a user driven strategy to recover the web", Institute of European Affairs 2007, referred to above, in footnote 6, p. 89.

work[82]. It can then be concluded that maintaining and up-dating a black-list would at least not amount to a negative economic impact on public authorities (and eventually tax-payers).

The Internet Watch Foundation in the United Kingdom, an organisation that is a key component in the UK's Industry/Police/Government partnership for tackling illegal content online, runs a black-list for illegal content. The estimated costs, in this case, include the development and building of the database, approximately 110,000 euros, as well as maintenance and regular up-grading costs of approximately 30,000 euros per year and human resources costs of about 60,000 euros per year.

But this list might also be co-financed, as it is the case of the black-list compiled and maintained by the Internet Watch Foundation. The Internet Watch Foundation relies on both private and public funding.

Therefore, if the black-list were to be financed by internet service providers to some extent, the costs indicated in the table above would slightly increase for all blocking systems save dynamic filtering.

5.2.3. Human rights impact

Direct impact on freedom of expression

This option implies a direct restriction of the freedom of speech. The extent of the negative consequences depends on the filtering system used. First of all, dynamic filtering clearly limits freedom of speech and access to information because it automates censorship, bypassing a black list created by humans and using instead a set of criteria of characteristics of the kind of material that should be censored. Freedom of speech and access to information would be subject to automated judgement calls determined by software designers. Under this system, a separate assessment of the necessity and proportionality of blocking a specific content could not take place.

The systems relying on a black list imply human intervention in the establishment and up-dating of the list. Therefore, the impact on the freedom of speech and access to information depends on two factors: first of all, how and by whom the content of the black-list is determined as well as on the legal remedies offered to web owners in order to challenge the decision of inclusion. Secondly, it depends on the degree of precision of the method of filtering. Collateral blocking, referred to above, may not only cause serious economic losses but necessarily involves a violation of the freedom of speech. Assuming that the manner in which the black-list was maintained and up-dated incorporated enough human rights' safeguards so that it did not involve any further restriction of freedom of speech than necessary, the table below reflects the impact of the different blocking methods on freedom of speech.

Filtering methods	Impact on freedom of speech

[82] Avoiding double-work is in fact the logic behind the project "Check the web" launched by the German presidency in close co-operation with Europol and aiming at centralising information on Islamic radical websites identified by Member States. It does not however intend to block any of the materials identified.

IP filtering	--
URL filtering	-
URL hybrid filtering	-
DNS filtering	--
Dynamic filtering	---

It should be noted that terrorist activists and supporters are increasingly using dynamic communication services through the Internet instead of static websites. Discussion forums, chat-rooms or instant messengers are therefore of growing importance. The access to these is often restricted. Therefore, if filtering methods were to be extended to such internet services, concerns regarding freedom of speech would increase. Moreover, this would add concerns as regards the right to privacy.

Indirect impact on right to life and right to integrity

Forbidding internet service providers to give access to material to block the dissemination of messages through the Internet aiming at public provocation to commit terrorist offences, recruitment or training for terrorism would have as its final aim the protection of human rights of potential victims, in particular the right to life and the right to physical and mental integrity, similarly to the offences introduced in the Council of Europe Convention on the prevention of terrorism. From this point of view, such prohibition has a positive, although indirect impact on human rights that should also be taken into consideration. However, the magnitude of such impact is rather moderate since it suffers from the same weaknesses identified when analysing the security impact of this option.

- Magnitude of the impact on the right to life and the right to integrity: +

It should be noted that the assessment of impacts resulting from option 2 and especially of its security impact, is based on two main circumstances: firstly, that forbidding internet service providers to give access to violent radical material will never allow law enforcement authorities to investigate, prosecute and convict the activists and supporters behind the dissemination of terrorist propaganda and terrorist expertise, and secondly, that existing technology suffers from important limitations, in particular current filtering methods can be circumvented and have been designed specifically for web access and do not function appropriately for most other Internet services including “peer-to-peer” communication technologies.

While the first of these factors will remain the same, future developments are likely to improve existing technology and may modify the statements made as regards the second factor. Concerning the possibility of supporting the development of new and more efficient filtering technologies, one should consider that: although filtering techniques may improve, the manner in which the Internet is built, the various services it provides and the amount of information it contains, makes it hardly possible to find a system with no gaps, no less because of constantly emerging new services. In this sense, the effort and costs of developing

and, especially, implementing such technology appear to be disproportionate to the results that would be achieved.

Furthermore, as stated above, it should be considered that discussion forums, chat rooms and instant messengers are increasingly used by terrorist activists and supporters. If filtering techniques were to be generally extended to postings and messages on discussion forums, chat rooms and instant messengers, concerns regarding the respect for human rights would considerably increase, not only with respect to freedom of speech but also the right to privacy. Necessity and proportionality make such interferences unjustified in a democratic society.

It appears more appropriate to focus on the surveillance and prosecution of terrorist activists and supporters behind the dissemination of terrorist propaganda and terrorist expertise. Therefore, funding projects and studies aiming at enhancing law enforcement authorities' capabilities and expertise to detect and analyse radical violent material as well as to trace their authors within the existing limitations and requirements of the legal framework is analysed below.

5.3. Option 3: Enhancing law enforcement authorities' capacities and expertise to counter the use of the Internet for terrorist purposes

5.3.1. Security impact:

Law enforcement authorities would receive the expertise of academics, would increase their own knowledge by specific training - including the development of technical and linguistic skills- and share their knowledge with law enforcement authorities of other Member States in order to develop and exchange efficient methods of monitoring. The results of the studies foreseen under this option could also advise the adoption of non-legislative measures to prevent the distribution of violent radical content on the Internet, including co-operation between NGOs and law enforcement authorities as well as to the development of methodologies and adapted technological tools to efficiently detect violent radical content on the Internet.

It can be concluded that law enforcement authorities would be empowered in order to detect and analyse violent radical content on the Internet. They would equally be in a better position to identify the individuals behind such content.

Pro-active policing of violent radical content on the Internet can provide for key information in order to understand the terrorist trends, anticipate terrorist actions and can provide for crucial data to prevent attacks. In this sense, enhancing law enforcement authorities' capacities and expertise to counter the use of the Internet for terrorist purposes is worthy to be considered as a standing-alone option. However, option 3 does not provide for a legal basis to open an investigation and prosecute the author of the messages of terrorist propaganda or terrorist expertise. In order to overcome these limitations, option 3 should be accompanied by adequate criminal law measures. Prohibitions such as those studied under option 2, would not be able to overcome such limitations since they do not constitute criminal law.

As regards the added value of European Union funding over national funding, it should be noted that the Commission plans to finance training and tools of national law enforcement, through trans-national projects that encourage sharing resources and avoiding double work. Moreover, financing through the Commission is efficient because it can exploit existing bodies and infrastructure (i.e. the Joint Research Centre to develop adequate software,

European Judicial Training Network for judicial training) it produces economies of scale (i.e. results of studies will be automatically shared) and encourages the division of tasks through trans-national projects.

- Magnitude of the impact on security: ++

5.3.2. Economic impact

Direct economic impact for public authorities and tax-payers

Direct costs deriving from this option would be mainly assumed by the budget of the Commission. According to the Council Decision of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme Prevention of and Fight against Crime, grants financing projects must cover at least 65% of the costs, the maximum being determined in each of the annual work programmes. In the case of the contracts of studies, the budget of the Commission would fully cover the costs. The total costs for the Commission in 2008 are estimated in 1.200.000 euros. In a second phase, studies might lead to the development of non-legislative measures, methodologies and tools to support law enforcement authorities' work. Further costs would be then generated, to be financed with charge to future Commission's budgets. The magnitude of these would be probably determined in the studies. Nevertheless, it can be concluded that the costs estimated for 2008 are not significant in the Commission's budget and that, although costs generated in a second phase may be more important, the development of non-legislative measures, methodologies and tools at EU level would be, by far, more efficient than if similar actions were undertaken at national level.

Under Article 5 of the Decision referred to above, the Programme is destined for law enforcement agencies, other public and/or private bodies, actors and institutions, including local, regional and national authorities, social partners, universities, statistical offices, non-governmental organisations, public-private partnerships and relevant international bodies. It follows that the remaining percentage of costs will be mainly financed by the public authorities of Member States. It must be noted that these costs can be analysed in two different ways. If the project was going to be developed even in the absence EU funding, the economic impact will imply only a change of funding source: EU funding instead of funding obtained from public authorities in the Member States. In this case, the Commission's support constitutes important savings at national level since the costs are distributed among a much bigger number of tax-payers. However, it should be assumed that in many cases EU funding is decisive since it covers most of the costs of the projects. Member States would then face additional, although quite limited, costs.

- Magnitude of the impact on economy: -

Indirect economic impact for internet service providers and consumers

Indirectly, the possibility of additional and more efficient surveillance of violent radical content might lead to further investigations on terrorist activities. It follows that internet service providers might be asked more often for traffic data under the data retention Directive. Therefore, indirectly, option 3 may lead to additional costs for internet service providers deriving from more extended use of the Data retention Directive. This is explained in detail below, under option 5. However, it is important to note that under option 3 law enforcement

authorities could only ask for location and traffic data if the dissemination of terrorist propaganda or terrorist expertise was a serious crime in the Member State where the internet service provider is based. Another possibility would be that, in the course of the investigation, another behaviour qualified as serious crime in that Member State is discovered.

- Magnitude of the impact on economy: -

5.3.3. Impact on human rights:

Direct impact on freedom of expression

Since the dissemination of messages of terrorist propaganda or terrorist expertise would not become illegal under option 3, no content circulating on the Internet could be censored and no individual could be prosecuted for this behaviour (unless this was already possible according to national law). It follows that option 3 does not introduce restrictions to freedom of speech. Similarly, concerning the right to privacy, further and more efficient surveillance on violent radical contents would not amount to any restriction. The absence of a legislative framework implies that the rules on the right to privacy and data protection at both EU and national level remain unchanged and that law enforcement authorities continue to respect the limits established by the law. Nevertheless, the human rights consequences will be the same as under option 1.

- Magnitude of the impact on human rights: -

Indirect impact on right to life and right to integrity

Enhancing the capabilities and expertise of law enforcement authorities has the final aim of protecting potential victims, in particular their right to life and their right to physical and mental integrity. In fact, such protection concerns all citizens, since experience shows that anyone is a potential victim. From this point of view, these practical measures have a positive, although indirect impact on human rights that should also be taken into consideration. The magnitude of such impact logically corresponds to the level of increased security achieved by this option.

As stated above, efficient detection and analysis of violent radical content should provide for crucial data contributing to successful investigations and prosecutions. In addition, law enforcement authorities conveniently trained and equipped would considerably improve their chances to trace and identify the individuals behind the dissemination of terrorist propaganda and terrorist expertise.

- Magnitude of the impact on right to life and to integrity: ++

5.4. Option 4: Urging Member States to sign and ratify the Council of Europe Convention on the prevention of terrorism

A political statement advising Member States to ratify the Convention might accelerate signatures and ratifications or even increase them. However, as a political statement, it would lack a binding character. It would be merely a political reinforcement of Member States' commitment to ratify the instrument, already expressed by their signatures thereof – with the exception of four Member States which have not signed the Convention. Even more, it should be considered that such recommendation has already been included in the list of actions of the

counter-terrorism action plan, advising Member States to sign and ratify various international instruments relevant to the fight against terrorism. From this point of view, a specific political instrument would represent even less of a change.

More importantly, assuming that the statement made a difference for the quick signature and ratification by all Member States, the harmonised incrimination of public incitement to terrorism, terrorist recruitment and training would remain outside the EU legal framework. Harmonisation would indeed be achieved through the signature and ratification of the Convention by all Member States. However, such harmonisation will not bring about the same results as legislation at EU level[83]. It can then be concluded that the impact of this option on security, economy and human rights will be quite similar to that of the status-quo option, assessed above.

---

[83] See under section 5.5.1 below the added value of the revision of the Framework Decision in relation to the existing Council of Europe Convention on the prevention of terrorism.

5.5. Option 5: Revising the Framework Decision on combating terrorism in order to introduce parallel offences to those foreseen under the Council of Europe Convention

5.5.1. Security impact

The revision of the Framework Decision on combating terrorism would explicitly incriminate the use of the Internet as a means of public incitement to terrorism, recruitment and training through the dissemination of bomb-making and other terrorist expertise, at least as long as it falls within the jurisdiction of the European Union. In addition to the impact on security resulting from option 1, option 5 would bring clear added value in terms of the application of harmonised rules on penalties and jurisdiction and ensure the application of related EU instruments. Moreover, it would guarantee a consistent approach between the Council of Europe and the European Union, putting the EU in a stronger position to request co-operation from third countries and private operators. These added benefits are detailed below:

Added value of the revision of the Framework Decision on combating terrorism vis-à-vis relying on the Council of Europe Convention on the prevention of terrorism:

1. The new offences would benefit from all previous harmonisation achieved by the European Union in the field of the fight against terrorism

    - Rules on penalties: Article 5 in relation with Article 6 of the Framework Decision on combating terrorism imposes a detailed regime on penalties and applicable particular circumstances for the offences mentioned in that Framework Decision. Most importantly, Article 5(1) contains a link to the European Arrest Warrant. This means that if the offences of public provocation to commit a terrorist offence, recruitment for terrorism and training for terrorism would be included in the Framework Decision on combating terrorism:

        (a) The new offences should be punished with imprisonment of at least one year. Other penalties, such as pecuniary sanctions, would not be sufficient.

        (b) The Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States would apply automatically to these three offences. If these offences were not included in Articles 1 to 4 of the Framework Decision, the application of the European Arrest Warrant would depend on whether the penalties' established by the Member States would meet the thresholds foreseen in the Framework Decision on the European Arrest Warrant which are a maximum custodial sentence of at least three years for certain serious crimes, including terrorism, and a maximum custodial sentence of at least one year with the possibility of refusal by the executing State if the behaviour is not a crime under its national law.

    - Rules on jurisdiction: Article 9(2) includes rules solving positive conflicts of jurisdiction, a set of criteria to determine jurisdiction when several Member States are competent. Such rules contribute to ensure fast and efficient prosecution of

trans-national terrorist offences. If the offences of public provocation to commit a terrorist offence, recruitment for terrorism and training for terrorism would be included in the Framework Decision on combating terrorism, the prosecution of the new offences would benefit from the application of these rules.

- The Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences: It ensures the provision of information concerning terrorist offences as laid down in the Framework Decision to Europol, Eurojust and the Member States when criminal investigations concerning prosecutions and convictions for terrorist offences which affect or may affect two or more Member States. Additionally, it foresees the setting up of joint investigation teams when appropriate to conduct criminal investigations into terrorist offences and obliges Member States to ensure that requests from other Member States for mutual legal assistance and recognition and enforcement of judgements in connection with terrorist offences are dealt with as a matter or urgency and are given priority. If the offences of public provocation to commit a terrorist offence, recruitment for terrorism and training for terrorism would be included in the Framework Decision on combating terrorism, its investigation and prosecution would benefit from such enhanced co-operation.

By introducing the new offences in the Framework Decision on combating terrorism, law enforcement personnel and judges are further empowered and investigations, prosecutions and convictions are facilitated. Public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism would be fought with the full EU arsenal of measures on terrorism.

1. The new offences would benefit from the advantages of third pillar instruments, in particular Framework Decisions, vis-à-vis international treaties and conventions

- Adoption by the Council implies an automatic obligation for Member States to adapt their national legislation. In contrast with the lengthy procedures to sign and ratify international conventions that can last for many years, Framework Decisions enter into force exactly as first pillar instruments do, most often the day of their publication in the Official Journal and set out a restricted period for implementation.

- Third pillar legislation becomes EU acquis: Therefore, it is compulsory for new Member States to adapt their legislation to existing Framework Decisions before joining the EU. By contrast, candidate countries are not obliged to adopt international conventions or treaties.

- Member States must notify the national measures implementing Framework Decisions to the Council and Commission. By contrast, such an obligation does not exist as regards the national measures adopted to implement international conventions or treaties.

- The correct and full implementation of Member States is evaluated as regards Framework Decisions: Framework Decisions generally foresee the establishment of an implementation report from the Commission and its assessment by the Council. Obviously, the European institutions are not empowered to assess the

correct implementation of international conventions and treaties by Member States.

- The European Court of Justice is entitled to interpret Framework Decisions via preliminary rulings. Sixteen Member States have accepted so far the authority of the European Court of Justice to deliver preliminary rulings as regards instruments of the third pillar. The European Court of Justice lacks any direct jurisdiction over international conventions and treaties.

- The European Court of Justice has stated that national courts are obliged to interpret national rules according to Framework Decisions. According to the Pupino case-law, national courts are required to interpret rules of national law, as far as possible, in the light of the wording and purpose of the Framework Decision.

By introducing the new offences in the Framework Decision on combating terrorism, Member States are expected to adapt their legislation earlier. Furthermore, European institutions could control the correct implementation and interpretation of the instrument.

1. The new offences affirm the position of the EU in the international context & vis-à-vis the private sector

- Co-operation with third countries and internet service providers is required to tackle public provocation to commit terrorist offences, recruitment for terrorism and training: Terrorism exceeds the territory and jurisdiction of the European Union, especially when it comes to the use of the Internet for terrorist purposes (i.e. 76% of the Islamist terrorist websites are hosted by internet services providers based in the United States). Therefore, international co-operation is required to tackle public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism. In particular, co-operation may be crucial in order to trace the terrorist activists and supporters behind such dissemination and, secondarily, disabling access to the relevant websites. A common ground shared by all Member States will strengthen the position of the European Union to achieve positive results in international fora such as the G8, the United Nations as well as through bilateral co-operation with relevant third countries. In addition, since all Member States are bound by EU legislation, the European Union could guarantee reciprocity. Similarly, the European Union would lack of legitimacy when seeking co-operation and agreements from internet service providers if public provocation to commit a terrorist offence, recruitment for terrorism and training for terrorism were not outlawed at European Union level.

- Outlawing public provocation to commit a terrorist offence, recruiting for terrorism and training for terrorism would be in line with the Communication on cyber-crime: The Communication refers to incitement to terrorism and glorification of terrorism when referring to illegal content[84]. It envisages certain actions in order to fight against illegal content, such as initiating and promoting dialogue with third countries on technical methods to fight illegal content as well

---

[84] Communication referred to above in footnote 19, p.

as on procedures to shut down illegal websites, also with a view to the possible development of formal agreements with neighbouring and other countries on this issue as well as developing EU-level voluntary agreements and conventions between public authorities and private operators, especially Internet service providers[85]. Such actions are not foreseen as regards harmful content.

By introducing the new offences in the Framework Decision on combating terrorism, law enforcement authorities could benefit in their investigations and prosecutions from stronger and more successful international co-operation. They could also request the disablement of access to a relevant websites hosted by an internet service provider based in a third country in those cases where this would not interfere or conflict with intelligence and investigation purposes.

- Magnitude of the impact on security: ++

5.5.2. Economic impact

Economic impact on public authorities and tax-payers:

There are no direct costs identified. However, the revision of the Framework Decision on combating terrorism might involve indirect costs. These costs would be similar to those that would stem from the signature and ratification of the Council of Europe Convention on the prevention of terrorism by all Member States, although they are likely to be marginally higher because of the link of the Framework Decision on combating terrorism with EU co-operation instruments referred to under the security impact. The new means to combat the terrorist threat would result in an increased co-operation of national law enforcement authorities both with industry and law enforcement authorities in other Member States. This should lead to improved results, which implies more successful investigations and more prosecutions than presently. However, further international co-operation and increased contacts with industry as well as increased prosecutions involve an additional work-load for law enforcement authorities.

The hypothesis of the additional work-load resulting from the revision of the Framework Decision on combating terrorism is in line with Europol's report TE-SAT 2007. The report states that the number of police investigations into terrorist propaganda seems small compared with the amount of material circulating on the Internet. The report clarifies that this is partially explained by the lack of legal basis for arrests or investigations using the Internet in this manner[86].

If the increased activity of law enforcement authorities required the allocation of further resources, these should come from the general national budget. Tax-payers would not necessarily assume higher taxes: the budget allocated to law enforcement and security may be increased at the expense of other public policies.

- Magnitude of the impact on economy: -

Economic impact on internet service providers and consumers:

---

85 Communication referred to above in footnote 19, p. 10.

86 See the EU Terrorism Situation and Trend Report 2007 of Europol, p. 21.

Option 5 would not involve direct costs for companies or consumers. Nevertheless, the same indirect costs as those detailed under option 1 have been identified.

- Magnitude of the impact on economy: -

5.5.3. Impact on human rights:

Direct impact on freedom of expression

Similarly to what has been explained under option 1 about the Convention on the prevention of terrorism, the inclusion of public provocation to commit terrorist offences, recruitment and training for terrorism under the Framework Decision on combating terrorism has a direct impact on the right to freedom of speech. This is especially true of the offence of public provocation to commit terrorist offences.

The analysis of this impact will therefore be very close to that of option 1. In fact, while the expected increase of investigations or prosecutions is relevant to figure out the impact of a criminal measure on security or on economy, the same does not apply to its effects on human rights. A measure must conform to human rights standards irrespective of the number of additional investigations or prosecutions stemming from it. A criminal measure which does not respect human rights does not become more acceptable because it is hardly applied in practice. Conversely, a criminal measure compliant with the ECHR does not become less acceptable because it is widely applied. In consequence, the main question is whether the restrictions of the freedom of speech deriving from the revision of the Framework Decision on combating terrorism would be covered by Article 10(2) of the ECHR. Insofar as the approach of the Council of Europe Convention on the prevention of terrorism is respected, including its safeguards and requirements, the revision of the Framework Decision on combating terrorism should comply with the ECHR.

In particular, public provocation to commit terrorist offences should require that two conditions are met[87] as explained in the explanatory report to the Convention on the prevention of terrorism. Firstly, there has to be a specific intent to incite the commission of a terrorist offence, which is supplemented with the requirements in paragraph 2 that provocation must be committed unlawfully and intentionally. Secondly, the result of such an act must be to cause a danger that such an offence might be committed.

The specific intent to incite the commission of a terrorist offence is of special relevance to ensure that the dissemination of information, opinions, views on terrorism and political conflicts as well as encouraging public debate on such issues is fully excluded from the scope of the revision of the Framework Decision on combating terrorism.

However, this option entails a risk linked to the negotiation process. Indeed, any Commission proposal to insert the definition of the offences of the Council of Europe Convention on the prevention of terrorism into the Framework Decision on combating terrorism is open to modifications during the negotiations by the Member States. Bearing in mind that the Council of Europe Convention on the prevention of terrorism is an outcome of intensive negotiations, it must be seen as the best compromise in this sensitive area aiming at enhancing the

---

[87] See the Explanatory report to the Council of Europe Convention on the prevention of terrorism, paragraphs 99 and 100.

efficiency of the fight against terrorism while ensuring the protection of fundamental rights. It follows that this option would require that all the institutions involved pay particular attention that the wording of the Council of Europe convention is maintained throughout the negotiation process.

- Magnitude of the restriction of freedom of speech: -

Indirect impact on right to life and right to integrity

The incrimination of public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism has as its final aim the protection of human rights of potential victims, in particular the right to life and the right to physical and mental integrity. In fact, such protection concerns all citizens, since experience shows that anyone is a potential victim. From this point of view, the amendment of the Framework Decision would have a positive, although indirect impact on human rights that should also be taken into consideration. The magnitude of such impact logically corresponds to the level of increased security achieved by the Convention. A higher level of security results in a lower the threat to the right to life and the right to physical and mental integrity of potential victims.

- Magnitude of the impact on right to life and to integrity: ++

6. SECTION 6: COMPARING OPTIONS

6.1. Summary table: costs and benefits

Options	Security impact	Economic impact		Human rights impact	
		Impact for public authorities	Impact for ISPs and consumers	Freedom of expression	Right to life integrity
Option 1 No policy change	+	-	-	-	+
Option 2 Filtering obligations	+	-			+
IP filtering			--	--	
URL filtering			--	-	

URL hybrid filtering			-	-	
DNS filtering			--	--	
Dynamic filtering			-/--	---	
Option 3 Practical support to LEA	++	-	-	-	++
Option 4 Political statement	+	-	-	-	+
Option 5 Revision Framework Decision	++	-	-	-	++

6.2. Advantages and drawbacks of the policy options

Policy options	Advantages	Drawbacks
Option 1: no policy change.	▪ Empowerment of law enforcement to fight new modus operandi of terrorists, including offences committed through the Internet. ▪ Respect of freedom of expression. ▪ Indirect protection of right to life and to integrity ▪ No need for new EU or EC legislation .	▪ Lengthy signature and ratification of the Convention by all MS. ▪ Rules of the Framework Decision on penalties and jurisdiction would not apply to the offences. ▪ Some EU co-operation instruments could not be used if the offences remain outside the EU Legal Framework. ▪ The EU would be in a weak position to request the co-operation of third countries and private sector ▪ Indirect costs for internet service providers ▪ Lack of control on national implementation. ▪ ECJ not entitled to deliver preliminary rulings ▪ EU counter-terrorist legislation outdated in relation to the UN and CoE. ▪ No solution for the lack of capacities and expertise of law enforcement authorities
Option 2: Forbidding internet service providers to give access to material to block the dissemination of messages through the	▪ Direct restriction of terrorist propaganda and expertise through the Internet. ▪ Possibility of building on	▪ Compulsory filtering does not allow for prosecution of the authors of the relevant material. ▪ Compulsory filtering does

Internet aiming at public provocation to commit terrorist offences, recruitment or training for terrorism.	existing experience on combating child pornography in certain Member States. ▪ Indirect protection of right to life and to integrity	not allow for the use of EU instruments for police and judicial co-operation in criminal matters. ▪ Filtering can be circumvented by experienced Internet users. ▪ Costs of implementation for internet service providers. ▪ Consumers are likely to be imposed additional charges. ▪ Risk of costs for companies and consumers in case of collateral blocking. ▪ Compliance with the ECHR is not guaranteed in all cases.
Option 3: Enhancing law enforcement authorities' capacities and expertise	▪ Addresses basic limitations of law enforcement authorities such as lack of technical or linguistic skills to counter the terrorist use of the Internet providing for practical solutions. ▪ Helps to understand terrorist trends, anticipate terrorist actions and prevent attacks. ▪ Stimulates the co-operation and sharing of knowledge between Member States so that they can benefit from existing efficient methods in others. ▪ Explores the development of methodologies and tools for more efficient detection and monitoring of violent radical contents	▪ The absence of legal basis which forbids or makes punishable public provocation, recruitment and training through the Internet implies that these forms of behaviour cannot be censored nor prosecuted. ▪ Strong skills and expertise would then be frustrated at the moment of taking action. ▪ All drawbacks of option 1.

	▪ Explores the possibility of involving NGOs that could support law enforcement authorities, acting as complaint hot-lines. ▪ Embodies the concept of economy of scale and prevents double working. ▪ Complements and builds on the German project "Check the web" ▪ No adoption of EU or EC legislation required. ▪ Respects freedom of expression ▪ Indirect protection of right to life and to integrity	
Option 4: Urging Member States to sign and/or ratify the Council of Europe Convention on the prevention of terrorism (through a political statement).	See Option 1	See Option 1
Option 5: Revising the Framework Decision on combating terrorism in order to introduce parallel offences to those foreseen under the Council of Europe Convention.	▪ Empowerment of law enforcement authorities to face new modus operandi of terrorists, including offences committed through the Internet ▪ Rules of the Framework Decision on penalties and jurisdiction would apply to the offences. ▪ Application of the European Arrest Warrant guaranteed. ▪ EU co-operation instruments linked to the Framework Decision could be used ▪ Full compliance with the	▪ Successful co-operation with third countries is not guaranteed. ▪ Indirect costs for internet service providers ▪ No solution for the lack of capacities and expertise of law enforcement authorities ▪ Conformity of amendment of the Framework Decision with the Council of Europe Convention of the prevention of terrorism at the end of the negotiations process is not guaranteed.

ECHR, as long as amendment of the Framework Decision fully corresponds to the existing human rights standards

- Control on national implementation
- ECJ entitle to deliver preliminary rulings
- Consistency between the UN, CoE and EU counter-terrorist policies.
- Strengthened position to seek co-operation from third countries and internet service providers
- No need to amend national legislation already adapted to the Convention

6.3. Summary table: check list of benefits

The table below compares the policy options against the same set of criteria, which detail relevant aspects of their impact on security, economy and human rights. It provides for a clear overview of the benefits of each policy option.

Table of symbols

The benefit is present	√
The benefit is absent	-

	Option 1	Option 2	Option 3	Option 4	Option 5
	No policy change	Filtering obligations	Practical support to LEA	Political statement	Revision FD
Security impact					

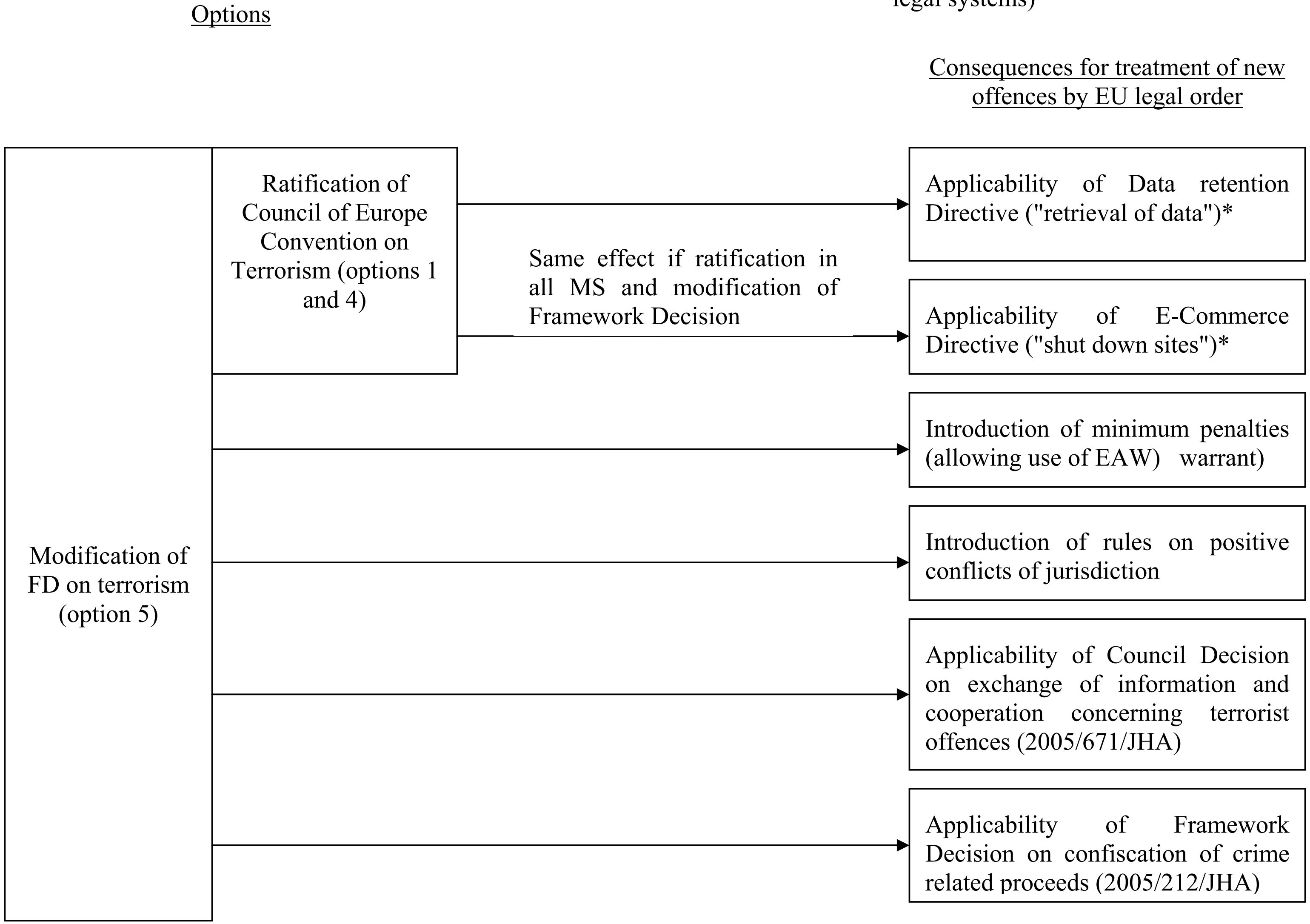
Legal basis for investigation and prosecution	√[88]	-	-	√	√
Increase expertise and capabilities of law enforcement authorities	-	-	√	-	-
Access to radical violent content on the Internet hindered directly	-	√	-	-	-
Application of rules on penalties and jurisdiction of the FD	-	-	-	-	√
Automatic application of EAW and other EU instruments	-	-	-	-	√
No need for lengthy signature and ratification process	-	√	√	-	√
Control on national implementation	-	-	-	-	√
ECJ interpretation via preliminary rulings	-	-	-	-	√
Consistency between the UN, CoE and EU counter-terrorist policies	-	-	-	-	√
Strengthened position to seek co-operation from third countries and internet service providers	-	-	-	-	√
Economic impact					
No substantial costs for private sector	√	-	√	√	√

88 Once all Member States have signed and ratified the Council of Europe Convention on the prevention of terrorism.

No substantial costs for national authorities	√	√	√	√	√
Human rights impact					
Compliance with freedom of speech	√	-	√	√	√
Protection of fight to life and to integrity	√	√	√	√	√

6.4. Introduction of public provocation to commit terrorist offences, recruitment and training for terrorism, also via the internet, as offences: An overview of options 1, 4 and 5.

(*The extent of the changes depends on the existence of comparable offences in the MS's legal systems)



6.5. Strengths and weaknesses of each policy option and preferred option

Option 1, no policy change, is not a true status-quo, since the Convention on the prevention of terrorism will bring about some positive impact on security, helping to tackle the issue of the use of the Internet for terrorist purposes. This option implies the empowerment of law enforcement to fight new modus operandi of terrorists, including offences committed through the Internet while fully respecting human rights and implies that there is no need for further regulation at EU level. However, full harmonisation will only be achieved once all Member States sign and ratify the Convention, which can last for many years.

Option 2, forbidding internet service providers to give access to material to block the dissemination of messages through the Internet aiming at public provocation to commit terrorist offences, recruitment or training for, i.e. compulsory filtering of terrorist propaganda and terrorist expertise content is the most extreme of the options examined. It presents the advantage of restricting directly the dissemination of the relevant materials through the Internet. However, it involves serious disadvantages, most importantly, it does not incriminate the behaviour of those producing terrorist propaganda and expertise nor does it fully guarantee compliance with human rights standards.

Option 3, enhancing law enforcement authorities' capacities and expertise, provides for practical solutions to overcome limitations of law enforcement authorities to detect and analyse the messages disseminating terrorist propaganda and terrorist expertise thought the Internet. It also helps them to identify the authors of such messages. The information obtained in this manner contributes to understand terrorist trends, anticipate terrorist actions and prevent attacks. However, it does not allow law enforcement authorities to investigate the dissemination of terrorist propaganda and terrorism expertise nor does it allow the prosecution of the terrorist activists and supporters behind it, since no legislation is adopted. In consequence, option 3 leads to a partial empowerment of law enforcement authorities, lacking the legal side.

Option 4, making a political statement urging Member States to ratify the Convention on the prevention of terrorism, does not present substantial differences from option 1.

Option 5, revising the Framework Decision on combating terrorism in order to introduce parallel offences to those foreseen under the Council of Europe Convention is the most advantageous option. This policy option is similar to option 1 as regards its impact on human rights, because it includes conditions and safeguards of the Council of Europe Convention on the proevention of terrorism, aiming to ensure the protection of human rights and fundamental freedoms. However, it implies important advantages such as the application of the rules of the Framework Decision on penalties and jurisdiction to the new offences introduced in the Framework Decision on combating terrorism. Additionally, it would guarantee the application of the European Arrest Warrant and allow for the use of specific EU co-operation instruments linked to the Framework Decision on combating terrorism in relation with the new offences. Furthermore, it brings about all advantages of EU legislation vis-à-vis international conventions and treaties.

Based on this analysis, it appears that the combination of options 5 and 3 would constitute the most effective policy to counter the new modus operandi of terrorist, in particular their use of the Internet as a means for public provocation to commit terrorist crimes, recruitment and training for terrorism, while fully respecting human rights.

Choosing option 5 does however not exclude option 4. The benefits of international instruments in the fight against the terrorist use of the Internet are beyond doubt and the importance of the Convention on the prevention of terrorism in this specific case is by no means underestimated or contested. The adoption of additional legislation along the same lines as those contained in the Convention intends to exploit all EU co-operation channels and instruments in order to fight the provocation to commit terrorist offences, recruitment and training for terrorism more efficiently, including their commission through the Internet. The revision of the Framework Decision on combating terrorism would therefore build on the Convention and boost its effects. A revised Framework Decision would also benefit from a widely ratified Convention operating at international level in a much broader forum than the EU and improving the chances of co-operation with third countries.

Option 3 appears to be the perfect complement to option 5. Law enforcement authorities do not only need the legal basis to counter the use of the Internet as a means to disseminate terrorist propaganda and terrorist expertise but also require the technical and linguistic skills as well as appropriate tools and methodology. Only with the appropriate training, the support of experts and efficiently equipped, will law enforcement authorities be able to make use of the new legislation. Similarly to option 5, option 3 as a stand- alone option would not provide for a complete solution to the problem. It would provide law enforcement with the expertise and capacity to detect, monitor and analyse the dissemination of terrorist propaganda and terrorist expertise as well as to trace the terrorist activists and supporters. However, law enforcement authorities could not open an investigation or prosecute such individuals. Accompanied by the legal measures foreseen under option 5, the capacities and expertise offered to law enforcement authorities under option 3 would be fully exploited. Only with adequate new legislation law enforcement authorities would be able to make full use of their additional capacities and resources.

7. SECTION 7: MONITORING AND EVALUATION

7.1. Monitoring of legislative measures (option 5)

Under Article 11 of the Council Framework Decision of 13 June 2002 on combating terrorism (hereafter 'the Framework Decision on combating terrorism'), the Commission has to establish a written report on the measures taken by the Member States to comply with this instrument.

In accordance with that Article, a report from the Commission as well as a Commission staff working paper associated with this report were adopted on 8 June 2004. A second report from the Commission also accompanied by a Commission staff working paper is currently under inter-service consultation and should been soon approved.

To be able to evaluate on the basis of objective criteria whether a Framework Decision has been fully implemented by a Member State, the two precedent written reports have applied some general criteria developed with respect to directives, such as:

1. form and methods of implementation must be chosen in a manner which ensures that the directive functions effectively with account being taken of its aims[89];

[89] See relevant case law on the implementation of directives: Case 48/75 Royer [1976 ECR 497 at 518].

2. each Member State is obliged to implement directives in a manner which satisfies the requirements of clarity and legal certainty and thus to transpose the provisions of the directive into national provisions having binding force[90],

3. transposition need not necessarily require enactment in precisely the same words in an express legal provision; thus a general legal context (such as appropriate already existing measures) may be sufficient, as long as the full application of the directive is assured in a sufficiently clear and precise manner[91];

4. a Directive must be implemented within the period prescribed therein[92].

If the Framework Decision on combating terrorism is revised, the evaluation system referred to above would also apply to the new provisions introduced.

7.2. Monitoring of non-legislative measures (option 3)

Article 13 of the Council Decision of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme Prevention of and Fight against Crime deals with monitoring. It ensures the monitoring of each of the actions financed by the programme. To this end, among other requirements, it obliges the beneficiary to submit technical and financial reports on the progress of work as well as a final report within three months of the completion of the action. In addition, it foresees the supervision and financial control of contracts and agreements resulting from the implementation of the Programme by the Commission, if necessary by means of on-the-spot checks, including sample checks, and audits by the Court of Auditors.

Article 15 of the same instrument refers to evaluation ensuring that the Programme is monitored regularly in order to follow the implementation of activities carried out there under. To this end, this provision foresees independent and external evaluation of the Programme as well as the submission, to the European Parliament and the Council, of an annual presentation on the implementation of the Programme; an interim evaluation report on the results obtained and the qualitative and quantitative aspects of the implementation of the Programme no later than 31 March 2010; a communication on the continuation of the Programme no later than 31 December 2010, and finally, an ex-post evaluation report no later than 31 March 2015.

Since the non-legislative measures envisaged in option 3 would be financed in the framework of this Specific Programme Prevention of and Fight against crime, Articles 13 and 15 would apply to these measures.

---

90 See relevant case law on the implementation of directives: Case 239/85 Commission v. Belgium [1986] ECR 3645 at 3659. See also Case 300/81 Commission v. Italy [1983] ECR 449 at 456.

91 See relevant case law on the implementation of directives for instance Case 29/84 Commission v. Germany [1985] ECR 1661 at 1673.

92 See substantial case law on the implementation of directives, for example : Case 52/75 Commission v. Italy [1976] ECR 277 at 284, See, generally, the Commission annual reports on monitoring the application of Community law, for instance COM(2001) 309.

ANNEXES

ANNEX I: REPLIES TO THE FIRST QUESTIONNAIRE ADDRESSED TO MEMBER STATES

1) Besides the necessary transposing provisions making incitement to commit terrorist offences punishable, does your country have (or plan to have) more detailed/further reaching provisions setting out restrictions or sanctions in relation to public provocation to commit terrorist offences, terrorist apology or glorification of terrorist offences or their authors?

And does your country have (or plan to have) more detailed/further reaching provisions in relation to the transmission of expertise on bomb or explosives-making, preparation of attacks, hostage-taking or other instructions for committing a terrorist offence?

Two Member States did not provide for any provision or answered very briefly because of their undergoing legislative modification in view of the ratification of the Convention on the Prevention of Terrorism of the Council of Europe.

The rest of the Member States referred to different criminal law provisions in their answers.

A first overview shows that every Member State but one have got or will have specific rules dealing with public dissemination of messages encouraging the commission of terrorist offences *(and often of other crimes). Although terminology is not at all uniform (i.e. "provocation", "instigation", "public incitement" etc.) we observe that there is a reiterative characteristic: they explicitly refer to publicly disseminated information. Often, the provision makes reference to dissemination in a meeting, via publication or sound and images supports. Some provisions deal specifically with "terrorist publications", including even a reference to the dissemination via the Internet. In other cases, the comments of the Member States explain that messages on the internet are included. Two Member States express theoretically this characteristic by saying that the recipient does not have to be previously determined. Actually, these two Member States stress that, by contrast with the general rules on incitement, in the relevant provisions the offence does not need to be determined beforehand either. In this sense, some Member States retain direct and indirect provocation. In five Member States, these provisions refer to the irrelevance of the subsequent commission of the offence or the actual incitement of the recipients of the message.*

Additionally, eight Member States have got or will have provisions condemning glorification or approval of terrorist offences *(and often of other crimes).*

Two Member States deal specifically with the denigration or humiliation of the victims. Two also refer to apology of terrorism or crime apology.

Three Member States referred to provisions explicitly covering the public dissemination of terrorist expertise. Six Member States have got or will have provisions on training or recruiting, mainly resulting from its adaptation to the Council of Europe Convention on the Prevention of Terrorism. *One Member State points out its provision on preparation of a crime, explaining that it comprises holding something especially intended to be used as an auxiliary means and that compiled information can be regarded as the said auxiliary means. Furthermore, it clarifies that the intent does not have to cover a specific terrorist offence.*

Another Member State refers to its general rules on complicity. Three Member States explain that the transmission of expertise would be criminalised under its penal code only if was done intentionally and the terrorist act was actually committed or attempted/planned. Two Member State link the dissemination of terrorist expertise to terrorist groups, making punishable the transmission information on terrorist targets. One Member State points out it has no specific provision concerning the transmission of terrorism expertise.

Six Member States mentioned provisions that are not part of their criminal law in their answers. Only one referred to aliens and associations law. The rest mentioned their media law as well as provisions on electronic communications or only the latter. Various highlighted that the dissemination of terrorist propaganda or terrorist expertise should be in principle fall within the scope of penal law or that media acts had not specific provisions concerning the said issues. The provisions forwarded prohibit incitement to hatred, endangering public order, security or important domestic interests and incitement to commit terrorist offences in the case of one Member State. It should be noted that such prohibitions, save in one case, go beyond the encouragement to the commission of a specific offence or approval of its commission. Indeed, they provide for wider prohibitions such as incitement to hatred or call for violence. Two Member States explicitly refer to their broader scope, indicating either that the threshold of incitement does not have to be trespassed or that cover behaviours that do not constitute a criminal offence.

Regarding their regulations on electronic communications, one Member State requires Internet Service Providers to be licensed, one Member State obliges them to delete illegal contents, *while one Member State stresses that they are not liable and another one notes that they are not subject to a general obligation to monitor.*

If so;

i) We would be extremely grateful if you could specify whether these provisions would constitute:

a) Criminal legislation

b) Media legislation

c) Other. Please, specify the branch of law in this case.

Please, tick the appropriate choice(s) and kindly give further details about the relevant legal instruments.

All Member States referred to criminal law. Additionally, six of them referred to non criminal law: *one referred to aliens and associations law. The rest mentioned their media law as well as provisions on electronic communications.*

ii) We would very much appreciate if you could indicate what problems have been encountered in implementing these provisions:

a) Problems in interpreting the criminal law provisions in question in full respect of the fundamental right of freedom of expression. We would be particularly grateful if you could provide us with legal opinions or national jurisprudence as to how the issue has been dealt with in your countries.

b) Resistance for commercial reasons from media, service providers or publishers.

c) Law-enforcement difficulties linked to the nature of the internet such as identifying the source of the illegal content or eliminating this illegal content.

c) Others. Please kindly provide further details in this case.

Please, tick the appropriate choice(s).

Some Member States declare not having had any problems concerning the implementation of the relevant provisions although some clarify that the rules are very recent and others explain that no cases of the relevant offences have occurred in their territory (Lithuania).

***Six Member States pointed out problems of enforceability derived from the extra-territorial nature of internet and, in particular, the fact that illegal contents are often hosted in third countries.** Some of them referred to cases where there is no international convention with the third country, in particular, convention of legal assistance. One Member State refers to the lack of harmonisation of illegal contents and data retention rules at an international level. There is also a specific mention of the United States and the first amendment to its constitution, which limits substantially the intervention of the authorities. One Member State describes the problem of determining the location, for which tracing the IP is required, as well as competent jurisdiction.*

***Two Member States refer to the contra-strategies used by terrorists**: encryption, which complicates the task of policemen, especially regarding the respect of investigation procedures in a democratic society; new technologies such as Skype or WI-FI; measures complicating the identification of the authors such as proxy servers, anonymizers or pre-paid SIM cards; the enormous number of connections in little time; the minor providers and their limited capacities, their cache memory being often switched off.*

One Member State mentions the high price of blocking techniques since minor service providers would be unable to apply them.

***Two Member States stress the need to cooperate with internet service providers** to access the information required to identify the authors of the messages while one of them refers to the lack of will from the side of webmasters of "risky" websites to cooperate with law enforcement authorities.*

Technical problems regarding monitoring the transmission of data among computers are as well mentioned by one Member State, which also refers to the problem of lengthy procedures.

One Member State refers to the problems of interpretation of the relevant provisions in full respect of the fundamental right of freedom of expression.

2) Does your country carry out any informal or administrative monitoring/suppression/restriction on public provocation to commit terrorist offences, terrorist apology or glorification of terrorist offences or their authors (e.g. blocking of websites, confiscation of materials, censorship etc)?

And does your country carry out such informal or administrative monitoring/suppression/restriction on the transmission of expertise on bomb or explosive-making, preparation of attacks, hostage-taking or other instructions for committing a terrorist offence?

If so,

i) It would be extremely useful if you could give details including which are the enforcement bodies (law enforcement authorities, other public administration bodies, private bodies/independent authorities representing media, service providers or publishers etc), their method of operation and the perceived benefits.

***Eight Member States refer to systematic monitoring of the Internet or systematic collection of information for terrorism prevention** pointing out in most of the cases that the authorities in charge are police authorities or intelligence services. Three Member States mention the authorities responsible for mass-media such as radio or TV, for contents disseminated through those media. **One Member State refers to an inspectorate responsible for the activities of electronic media within the Ministry of Economy**. Eight Member States explain that police authorities act on a case by case basis further to judicial orders or under supervision of the competent attorney. One Member State states it does not carry out any measures as those referred to in the question.*

ii) We would very much appreciate if you could indicate what problems have been encountered in carrying out this system:

a) Problems in interpreting the criminal law provisions in question in full respect of the fundamental right of freedom of expression. We would be particularly grateful if you could provide us with legal opinions or national jurisprudence as to how the issue has been dealt with in your countries.

b) Resistance for commercial reasons from media, service providers or publishers.

c) Law-enforcement difficulties linked to the nature of the internet such as identifying the source or eliminating the illegal content.

d) Others. Please, kindly provide further details in this case.

Only one Member State answered, indicating the different process to close-down a site with illegal content depending on its location: national territory, UE Member State or third country. In last case, everything would depend on a principal problem the problem of sites

hosted in a third country, as the success would depend on the cooperation agreements with the country in question.

Some Member States, however, had already answered this question in their replies to question 1(ii) which is indeed closely connected.

3) Does your country maintain data or studies on public provocation to commit terrorist offences, terrorist apology or glorification of terrorist offences or their authors that it would be willing to make available for the elaboration of the proposal for a modification of the Framework Decision of 13 June 2001 on combating terrorism or for the development of further EU legislation in this area? The Commission will respect any security restrictions specified on the publication and dissemination of such information.

And does your country maintain such data or studies on the transmission of expertise on bomb or explosives-making, preparation of attacks, hostage-taking or other instructions for the commission of a terrorist offence?

Most Member States stated that they do not have specific or separated data or studies on the transmission of terrorist propaganda as well as bomb-making and other terrorist expertise. *Yet, one Member State explained that Service of Postal and Communication Police stores data and information concerning the results of investigation and monitoring of communication systems and services on the relevant subjects. Another Member State referred to its action plan against radicalisation including a contact point "Internet". Finally, one Member State pointed out a data base specifically on terrorist offences that would be willing to make available.*

4) Considering the unique position of the EU to help tackle what is often a cross-border issue, with protagonists in different countries, and information flowing freely between different jurisdictions, does your country consider there is a need for more detailed/further reaching legislation dealing with both terrorist propaganda and the transmission of bomb or explosives-making expertise ?

The answers given by Member States have been compiled in the tables below.

Need to revise the Framework Decision	*No answer/open answer*	*No*	*Yes*	*Yes only regarding terrorist propaganda*	*Yes only regarding bomb-making and other terrorist expertise*
Member States	*3*	*7*	*5*	*1*	*2*

If so;

i) It would be extremely useful if you could indicate which of these options you think is preferable:

a) Limit the scope of this legislation to the circulation of terrorist propaganda and transmission of expertise on bomb or explosives-making, preparation of attacks, hostage-taking or other instructions for the commission of a terrorist offence through the internet since the use of this channel for terrorist purposes is undoubtedly much higher than that of any other media and very often, there is not appropriate legislation covering the internet.

b) Extend the scope of the legislation to the circulation of terrorist propaganda and transmission of expertise on bomb or explosives-making, preparation of attacks, hostage-taking or other instructions for the commission of a terrorist offence through all media, including the press and broadcasters, assuming that the study of Member State's legislation on the latter makes us conclude that there is a need to modernise these rules in order to adapt them to present day forms of terrorism.

options	*None of the given options/open answer*	*a*	*b*
Member States	*9*	*3*	*6*

ii) We would be extremely grateful if you could tell us whether your country considers that the Framework Decision of 13 June 2001 on combating terrorism should be modified so that public provocation to commit terrorist offences, terrorist apology or glorification of terrorist offences or their authors are punishable in all Member States.

If so, please kindly indicate which of the following options is preferable in your view:

a) Make punishable the public provocation directly advocating a specific terrorist offence.

b) Make punishable the public provocation to commit terrorist offences in line with the Convention on the prevention of terrorism of the Council of Europe (directly or indirectly advocating terrorist offences with the risk that one or more offences can be committed).

c) Make punishable the apology/glorification of terrorism.

Options	*None of the given options/open*	*a*	*b*	*c*

	answer			
Member States	*13*	*2*	*3*	

iii) It would be extremely useful if you could indicate whether your country considers that the Framework Decision of 13 June 2001 on combating terrorism should be modified so that transmission of expertise on bomb or explosives-making preparation of attacks, hostage-taking or other instructions for the commission of a terrorist offence is punishable in all Member States.

If so, please kindly specify which options would be preferable in your view:

a) Make punishable all transmission of such expertise.

b) Make punishable only the transmissions made with terrorist intent.

c) Impose criminal liability only on the transferor.

d) Impose criminal liability only on the transferee.

d) Impose criminal liability on both of the parties involved.

Options	*None of the options given/open answer*	*a*	*b*	*c*	*d*	*e*
Member States	*13*	*4*			*1*	

ii) Does your country consider that it would be preferable to address the issue of terrorist propaganda by using first pillar legislation so that public provocation to commit terrorist offences, terrorist apology or glorification of terrorist offences or their authors would not be punishable under criminal law but restricted or sanctioned under internal market and/or media legislation?

And does your country consider the use of such legislation preferable to address the issue of transmission of bomb or explosives-making expertise through the media?

The vast majority of Member States agree that it would be preferable to address the subject through legislation under the third pillar.

5) Apart from the possibility of more detailed/further reaching legislation to address the issues of terrorist propaganda and transmission of bomb or explosive-making expertise, would your country like to see the EU, with Europol in the operational sphere, play a greater role in coordinating the efforts of the Member States in order to develop joint monitoring of the internet, co-ordinated notification of and closure of websites, unified negotiating position in relation to internet service providers or any other initiative in this area? If so, could you please specify which role?

All Member States stress the importance of coordinating the efforts of Member States in fighting the use of the Internet with terrorist purposes. *Eight Member States refer to the co-operation with Europol, two of them also mention Eurojust and one of them Sit-Cen. Several express their support to the Germany's Check the Web proposal.*

One Member State highlights the role of the EU might have in co-operating with Internet Service Providers and negotiate with third countries, in particular with the USA, where most of the Internet sites are hosted. It also points out the need to reflect, at an international level, on the sensitive material often exposed on Internet sites by administration and particulars as well as on the exchange and sale of e-bay.

ANNEX II: REPLIES TO THE SECOND QUESTIONNAIRE ADDRESSED TO CIVIL SOCIETY, INDUSTRY AND MEDIA

As a preliminary remark, it should be noted that eight of the answers have not followed the questionnaire but have given a **general reply** expressing their main concerns or raising their interests.

In this sense, **the following recurrent points should be highlighted:**

Regarding Media Associations

- **Concern for the respect of human rights and, in particular, freedom of speech**: by attempting to increase security, the EU can undermine civil liberties and damage the basic role of the media in democratic societies. Fearful of terrorism, the EU might adopt measures leading to censorship or simple ignorance of the facts on the ground.

- **Need to return to defence of human rights, reinforce freedom of speech and strengthen quality and ethical journalism.** The weapons against terrorism are reason, information, debate and wisdom. To achieve this objective, we need free and responsible media.

- **The EU should strictly respect the editorial independency of the media.** There should not be government control on editorial content. State-led measures disguised as self-regulation will not be supported.

- **The EU should not introduce any new measures on freedom of expression and information in the media unless strictly necessary and proportionate in a democratic society.** It should check carefully whether existing regulation or measures are not enough. In particular, **the EU should refrain from adopting measures equating media reporting on terrorism with support for terrorism.** Too widely formulated provisions on incitement might end up applying to journalists and media. Special concern causes in this sense the criminalisation of glorification of terrorism.

- **No need to define "incitement" at EU level.** The Framework Decision should be confined to setting the goals and leave specific measures and means to the Member States.

- **Need to enhance human and technical means available for the detection and elimination of that kind of threat while respecting Rule of Law and the Human Rights.**

Regarding Associations of internet service providers and telecommunications operators

- According to the e-commerce Directive, **Internet Service Providers do not disseminate information but are mere conduits**, not liable for information transmitted over the services they provide. Similarly, under the same instrument, they are not liable for the information they host unless they have actual knowledge of illegal material and fail to take steps to remove it.

- **A concern regarding the eventual intention of the EU to use blocking techniques to tackle terrorist contents.**

- **The decision regarding the legality of contents disseminated through the Internet should not be left to Internet Service Providers.**

- **Offer for further dialogue and co-operation to develop feasible, appropriate and effective tools to fight terrorist contents on the Internet.** Possibilities of public-private partnership would include further training and support for law enforcement by Internet Service Providers and development of technology directly assisting law enforcement authorities in their work.

<u>Technical points</u>

- The Convention on the Prevention of Terrorism of the Council of Europe builds on the case-law of the European Court of Human Rights and contains several clauses of safeguard of freedom of expression, i.e. Articles 12 and 21, ensuring its full compliance with human rights.

- Incitement to terrorism should be a criminal offence only where there is a criminal intention and the speech concerned causes the commission of a terrorist act or the imminent risk of such a commission.

<u>Concerning the **detailed answers**, they have been compiled below:</u>

1. How would you assess the effectiveness of Article 4 of the *Framework Decision on Combating Terrorism,* and of its implementation in Member States, against inciting, aiding or abetting a terrorist offence as defined by the Framework Decision itself?

One answer notes that effectiveness must be seen as preventing terrorist activity or preventing dangerous dissemination of terrorist materials, yet respecting the freedom of speech of individuals and the media to be able to report on the events.

Other reply points out its complexity and danger as verbalising ideas might become a crime.

Another one stresses that the scope should not be extended to include conducts such as apology, encouragement, justification or glorification of terrorism. Broadly worded offences may have a chilling effect in inhibiting a constructive debate.

2. Could you provide any information or examples that in your view demonstrate how Article 4 fails to cover certain terrorist offences or, on the contrary, information or examples demonstrating how this provision applies to cases which should not be considered as a terrorist offence?

According to one of the answers, the main point is not how to legislate, but how to apply the law. It refers to the example of a Portuguese court which failed to prevent a terrorist threat, releasing a terrorist suspect, who was only condemned to leave the country.

Another reply shows its concern about the description of the intentional element of a terrorist offence under Article 1 of the Framework Decision "unduly compelling a Government or an international organization to perform or abstain from performing any act" since "any act" might cover an act of publishing. Nevertheless, it notes that there have not been specific problems up-to-date.

Otherwise, it is noted that too wide competences of criminal investigation may hinder journalists in their profession.

3. What are your views with regard to the fact that there is no legal definition of incitement in the Framework Decision?

***The lack of definition of incitement in the Framework Decision is generally not regarded as problematic.** Different reasons are given: the Framework Decision does not apply directly but must be implemented by Member States so that national law can provide for legal certainty; a case-by-case system, sufficiently open for the judge is considered preferable to too exhaustive provisions, or there is no need for a uniform definition of incitement, generally understood as public instigation.*

One answer explains that properly defined and applied, offences of incitement to acts of terrorism are sufficient to criminalise indirect incitement, without resort to broader offences of apology, glorification, justification or encouragement of terrorism. It adds that if "incitement" in Article 4 were to be broadly defined to include glorification, justification or encouragement of terrorism then this, combined with the wide definition of terrorism and the range of terrorism offences to which it would apply, would make the scope of the prohibition under the Framework Decision highly indeterminate, in breach of the principle of legality, and would risk disproportionate or discriminatory interference with rights to freedom of expression. In order to safeguard against such over-broad definitions at a national level, an express clarification that incitement under Article 4 should be limited on the basis of the Johannesburg Principles would be beneficial.

4. a) What are your views with regard to Article 5 of the recently adopted Council of Europe Convention on the Prevention of Terrorism (2005) in which the public provocation to commit a terrorist offence is defined as: "the distribution or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed"?

b) Please, if possible, complement your answer by assessing the impact that the implementation of such a provision might have on you as an industry, association, organization or body concerned, or the impact that it might have on civil society in general.

Two replies noted that the Convention on the Prevention of Terrorism of the Council of Europe was elaborated bearing in mind the relevant case-law of the European Court of Human Rights and after conducting a survey of relevant national law and practice on incitement. Furthermore, it contains several clauses of safeguard of freedom of expression, i.e. Articles 12 and 21, ensuring its full compliance with human rights.

One of the replies points out that, in order to effectively protect freedom of expression, the Article 5 requirement that conduct should cause a "danger" of a terrorist offence should be interpreted as requiring a real and imminent risk of such an offence in the particular circumstances of the case, rather than a mere abstract danger.

One answer fears misinterpretations of the provision having a negative effect on the media. Another answer goes further, considering that a provision that criminalises the behaviour of transmitting a "terrorist" message on the sole basis that it causes a danger jeopardises freedom of information. This reply also insists on the role of media to disseminate knowledge on terrorist deeds so that a critical debate on terrorism can take place.

One reply notes that the resource to propaganda has shown as one of the most efficient weapons of terrorist groups as Al-Qaeda, that must be fought by all the means. This task of prevention implies the existence of permanent teams on the Net, which can interact in the sites of propaganda, identifying authors and places of diffusion.

5. a) What are your views with regard to the analysis made in the Explanatory Report to the above mentioned Council of Europe Convention that the above-quoted provision would cover:

   - dissemination of messages praising the perpetrator of an attack
   - denigration of victims
   - calls for funding terrorist organisations
   - other similar behaviour

b) Please, if possible, complement your answer by assessing the impact that the implementation of a provision explicitly forbidding the dissemination of one or more of the abovementioned messages might have on you as an industry, association, organization, or body concerned, or the impact that it might have on civil society in general.

One of the replies notes that such acts are committed with intent to incite acts of terrorism, and where they lead directly to an act of terrorism or the imminent risk of such an act, they can legitimately be criminalised. Conversely, however, where such acts are not committed with the requisite intent, and do not lead to an act of terrorism or the immanent risk of such an act, their criminalisation would not serve a pressing social need and would risk non-compliance with Article 10 ECHR.

One reply opposes to such interpretation and wonders who is held responsible if someone posts a message on the website of a media company. It also notes that "other similar behaviour" it too a wide expression.

A last reply indicates that "denigration of victims" and "calls for funding terrorist organisations" are punishable in Germany. It adds that "messages praising the perpetrator of an attack" should not be punished if disseminated in the context of an objective, critical report whose sole basis is to meet the public's request for information.

6. Are there any other situations that, in your view, could also be covered by a provision of this type addressing indirect incitement to commit terrorist offences? Are there any situations that, in your view, should not be covered by a provision of this type?

One reply considers that the situations in which indirect incitement to acts of terrorism is criminalised, should be limited to situations where there is a subjective intent to incite, and an imminent risk that an act of terrorism will result from the incitement. Where these criteria are fulfilled, and where the offence is based on a determinate and adequately circumscribed definition of terrorism, and is applied in a way that is non-discriminatory, there is likely to be compliance with human rights law. It further enumerates ***five situations that should be excluded from any provision on incitement to terrorism:***

• ***Explanation of circumstances surrounding the resort to terrorist acts*** *– for example, expression of understanding of the desperation of those who resort to suicide bombing in response to a repressive regime;*

• ***Teaching and academic or media debate on the political situation*** *in countries where there is armed opposition to the government, or concerning ideologies grounding terrorist movements;*

• ***Debate within immigrant communities of the political situations in home countries where there is internal conflict or terrorist violence,*** *including constructive debate on how to counter an oppressive or undemocratic regime;*

• ***Dissemination – including by the media and by human rights organisations – of information on violations of human rights by a government****, or criticism of a government for violations of human rights, for example those committed in suppressing a terrorist threat or in the course of an internal armed conflict;*

• ***Media or NGO reporting of statements by terrorist groups,*** *where such reporting is not intended to incite terrorism.*

Another reply states that any prevention of general news reporting would have a grave effect on the freedom of the press. Any attempt by governments to silence critical voices is a concern. The situations that should not be covered by a provision of this type are: news gathering, investigation and reporting, editorial comment. A similar reply adds teaching to these forms of behaviours not to be covered by this kind of provision.

One answer stresses the existence of such indirect attempt in nowadays terrorist activity.

7. Could you provide any information/analysis/assessment on the compatibility between freedom of expression and the notion of incitement, whether direct or indirect, to commit terrorist offences? Would you have any information/analysis on concrete cases examined by the competent authorities or Courts?

One of the answers points out the necessary respect of the principle of legality, the principle of proportionality and the absence of discrimination. It further notes the importance of the authoritative standards set out in the Johannesburg Principles on National Security, Freedom of Expression and Access to Information. They should provide the benchmark for offences of incitement to acts of terrorism, including European law. Principle 6, in particular, states that:

"Expression may be punished as a threat to national security only if a government can demonstrate that:

(a) the expression is intended to incite imminent violence;

(b) it is likely to incite such violence;

(c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence."

Another answer stresses that it is an extremely delicate frontier. It points out that it is necessary to decide in a case-by-case basis, taking into consideration the context.

One answer claims that It is not always possible for reporters to fully foresee the results that their reporting will have. This is where the public interest test comes in, twinned with editorial responsibility. Freedom of expression should be guaranteed for the press media in all circumstances. Journalists do have a right to inform the public about events that are outlawed, or indeed inform on information that is restricted if it is in the public interest to do so.

Another answer notes that journalistic activity cannot be considered as direct or indirect incitement unless especial personal circumstances provide evidence of this.

8. a) Could you provide any information/analysis/assessment on how Member States' legal systems deal with the question of the glorification and/or the apology of terrorism or terrorist offences?

   b) If, for instance, a specific incrimination exists, how is such behaviour defined and how is the compatibility with freedom of expression guaranteed?

One association notes that the treatment varies widely from Member State to Member State and it is difficult to generalise. It claims that several of its members would have had problems with the national legislation relating to terrorism. It emphasises how difficult it would be to develop a definition of glorification of terrorism at a EU level and the associated difficulties it would entail for freedom of speech.

One reply expresses concern at the emerging trend for national implementation measures to go further than is required by Article 5 of the Council of Europe Convention and thereby impose unnecessary and unjustifiable restrictions on rights to freedom of expression. It adds that the political invocation of international law obligations to prevent terrorism as a justification for measures restrictive of human rights, to an extent that is not justified by the terms of international agreements on terrorism, is of particular concern.

One answer states that the Occidental legal systems have become heavy and slow. The current legislation referred to crimes related to terrorist activity constitutes some innovation in a controversial field where the human rights of the suspects are in fact respected.

Another reply explains that every criminal act have to be interpreted in accordance with the constitution.

9. a) Could you provide any information/analysis/assessment on how Member States' legal systems deal with the question of transmission of bomb-making or other terrorist expertise, as well as any exceptions in pre-defined legitimate circumstances?

   b) If, for instance, a specific incrimination exists, how is such behaviour defined and how is the compatibility with freedom of expression guaranteed? Kindly provide concrete examples if possible.

One answer stresses that the mere act of publishing information about the ingredients of such devices should not be considered as a criminal act. It should not be illegal for the media to show film footage from terrorist camps or on how to make bombs in the interests of reporting.

Another reply points out that, more than the legal treatment, what matters is the means to identify and consequently deactivate such sources of information.

A last reply details that if the action serves the purposes of art, science, research, teaching or reporting on current affairs or past events, it does not constitute a criminal offence according to German law.

10. Which one or more of the acts in the list below would you qualify as "other terrorist expertise"? Should you think that certain acts should be added to or removed from the list, kindly specify them and motivate your answer.

    - in general, terrorist manuals or handbooks
    - instructions on how to conduct hostage-taking
    - instructions on how to create a terrorist cell
    - recipes for making poisons
    - instructions on how to make or utilise terrorist weapons (eg CBRN weapons) or a weapon of mass destruction

One association agrees with all elements on the list but points out that may be other that are unknown.

Another association states that it is important not to be over-reaching to such an extent that people don't receive information that is factually useful for them to be able to inform themselves against the dangers that are existing.

11. Please, if possible, assess the impact that the implementation of a provision explicitly forbidding the transmission of bomb-making expertise or one or more or the abovementioned categories of "terrorism expertise" has or might have on you, as an industry, organization or body concerned, or the impact that it might have on civil society in general.

The effects, points out one answer, depending on the way in which the provision is worded, could hinder the freedom of the press to report on terrorist acts, or to report on terrorist cases before the court. It would be unwise to enter into the territory of banning the factual element of information to the public, at the risk of being too restrictive of public information and infringing the right to receive information as protected by Article 10 of the European Convention on Human Rights.

Another answers states that, since the dissemination of "terrorism expertise" may have extremely pernicious consequences, the detection and close down of websites containing such information is an urgent need.

A last reply indicates that media in Germany are already bound by constitutional order, general legislation and rules for the protection of youth and personal honour, so that their activities are already limited by criminal law. In addition, journalists are adequately bound by voluntary undertakings to take responsible action. As for the danger that media involuntarily promote terrorist aims, such indirect effect of reporting could only be completely prevented by unacceptable methods that would significantly restrict the use of the Internet and completely prohibit reporting on terrorism.

12. Could you provide any information/analysis/assessment on whether Member States'legal systems differentiate between various types of media in relation to inciting tocommit, aiding or abetting terrorist offences and restricting the transmission of bomb-making or other terrorist expertise?

Another reply explains that to their knowledge, newspapers are not treated differently to other media and adds that it cannot support any extension of police powers into the realms of preventing publication of news reporting whether electronically or in print.

One reply points out Great-Britain as the example of how working jointly, authorities and Media, can keep the society informed.

13. Keeping in mind the generic nature of Framework Decisions of the EU, how would you view the possibility of amending article 4 of the EU Framework Decision on Combating Terrorism in order to achieve the following:

    - strengthen the prevention of incitement, aiding and abetting commit terrorist attacks, particularly via the internet

    - avoid unjustified or abusive incrimination of acts or behaviour which should not be considered as terrorist offences

One answer stresses the two important points are the human and technical means available for the detention of that kind of threat and always respect Rule of Law and the Universal Declaration of the Human Rights.

Another replay points out they would accept amendments that avoid as far as possible any unjustified or abusive criminalisation of acts or behaviours that should not be considered as terrorist offences, especially where this endangers the media investigation, news gathering, reporting, exchange of comment, opinion, taste, or suchlike on any press media platform.

Another answer states that the Decision 7/06 of the OSCE Ministerial Council points out an important first step with regard to online content, calling on participating States "...when requested to deal with content that is illegal under their national legislation and is hosted within their jurisdiction, to take all appropriate action against such content and to co-operate with other interested States, in accordance with their national legislation and the rule of law, and in line with their international obligations, including international human rights law."

Another reply explains that German criminal law the distribution of written communications is on a par with the distribution of sound and image carriers, data storage devices, illustrations and other depictions and is sanctioned in the same way as incitement to criminal offences via the Internet. It is therefore unnecessary to specifically include actions that take place via the Internet. In addition, this replies comments that unfounded suspicion is adequately countered in that incitement is only punishable if it takes place intentionally.

14. How would you address the particular difficulty of implementing Article 4 of the Framework Decision with respect to internet content?

The replies stress that the solution does not lie in the updating of the Framework Decision in terms of its detailing but it mainly concerns finding sophisticated technical solutions that would enable fulfilment of the Framework Decision. The question should thus be dealt at the level of assignment of the human and technical resources.

A last reply notes that German Internet law provide for a differentiated system that responds to the Internet-specific difficulty of foreign content being stored on own servers or on an access provider's servers without the provider being able to thoroughly check all the content. The Framework Decision, the reply continues, should be therefore confined to setting goals and should leave specific measures and means to the Member States.

15. Please feel free to provide any further comments you might have on the subject.

Two remarks should be noted:

- *The need to safeguard the current occidental legal system and the focus on technical and human means available for prevention and combat of terrorism.*

- *The media should never be encouraged by policymakers to practice any kind of self-censorship.*

ANNEX III: REPLIES TO THIRD QUESTIONNAIRE ADDRESSED TO EUROPOL, CEPOL AND EUROJUST

As a preliminary remark, it should be noted that most answers have not followed the questionnaire but have given a **general reply** expressing their main concerns or raising their interests.

In this sense, **the following recurrent points of the replies from Eurojust and the European Judicial Network[93] should be highlighted:**

- **The present subject certainly constitutes a political urgency.** Terrorist suspects are active on the Internet, disseminating their message, taking part in chat-forums, using email and downloading terrorist or radical material. In major investigations an enormous amount of digital material has been seized.

- **Need for translators and technical expertise for monitoring radical material on the Internet- Need for enhancing instruction and training of law enforcement authorities.** Presently, law enforcement authorities lack of capacity and expertise, processing and interpreting the radical websites in question is an enormous time-consuming and labour-intensive process, because of the quantity of the material and the languages in which the documents have been established. Experiences on the field show that for the successful implementation of this task it is necessary (thorough) knowledge of the Arab language and culture. The capacity at European level for interpreting radical websites should be improved. Attention should also be given on the possibilities of innovative detection methods for the internet surveillance.

- **Need for proper legislation so that law enforcement authorities are not hindered by lack of legal provisions.** Outlawing internet websites supporting terrorist views would be a good step forward (designating as terrorist crimes the offences of sedition, dissemination of seditious writings and fomenting hatred). The dissemination or possession of bomb-making and similar expertise in itself is not considered a criminal offence in itself in several Member States but needs the intention of the transferor to facilitate to commit a crime or offence which the transferee should plan or commit. It might be assimilated to child pornography and become a criminal offence in itself (designating as terrorist crimes the possession and dissemination of terrorist material such as instructions for making bombs).

- **Particular difficulties to trace suspects when the radical material is hosted in countries lacking appropriate legislation.** Sometimes, these countries lack of ability or willing and are reluctant to prosecute or extradite a certain individuals.

- **Need to respect human rights and freedom of speech in particular.** Certain measures are bound to be more intrusive and would sometimes limit individual rights but their impact will be limited by their legality, proportionality and necessity in a democratic society.

---

93 European Judicial Network has not sent a unified answer but several replies from three of its Members.

- **Interventions on the Internet Notice and take down of radical internet sites and/or radical material remain laborious until now.** In addition, after the radical thinking and terrorist material is taken down from a website, it re-appears very easily on another website. A more universal application of the Cyber-crime convention may improve the success of prosecutions.

- **Need of dialogue with internet service providers,** trying to bring about agreements to improve detection and tracing of radical material and its authors. Importance of the Data retention Directive, which requires Internet Service Providers and telecom operators to keep details of their subscribers' communication for up to two years.

Concerning the **detailed answer forwarded by Europol, it has been summarised below**:

1. How would you assess the ability of law enforcement authorities in Member States and your own organisation if applicable to respond to the use of new technologies and especially of the internet for terrorist purposes?

The ability of law enforcement authorities in Member States to respond to the use of new technologies and especially of the Internet for terrorism purposes is not homogenous and depends on several factors:

- ***Evaluation of the threat directly related to each Member State's experience in the field of terrorism.*** *There is an important difference between those who have and those who have not experienced national terrorism.*

- ***Law enforcement authorities' action against propaganda website is very limited due to the fact that most of these are located outside the remit of the national legislation.*** *Websites have such a short lifespan that by the time a legal action is brought through the international legal channels, they will have disappeared.*

Factors to be considered also include *the diversity of policing within the Member States regarding:*

- the legal mandate of concerned law enforcement authorities
- the monetary, technical and personal resources available
- the quality & training of respective law enforcement officers
- the technical equipment & standards at their disposal
- the language & translation capabilities of the staff
- the standardisation of information exchange
- the handling, processing, storing & forwarding of data

2. How would you assess, in particular, the ability of law enforcement authorities in Member States and your own organisation if applicable to respond to the dissemination of terrorist propaganda and bomb-making and other terrorism expertise through the internet? Do you

consider that this ability could improve by modifying the existing legal framework and the Framework Decision on combating terrorism in particular?

The ability of law enforcement in Member States to respond to the dissemination of terrorism related information via the Internet is very limited. *Their task depends on codified constitutional and/or national law. While the administrators of the websites are most often outside the EU and thus out of reach, this leaves law enforcement with the issue, at MS level, of policing the individual use on a local computer and perhaps the network to which the system is connected.*

Besides, resources are scarce. *Therefore Member States critically need to evaluate and direct their efforts properly.*

The use of the Internet for terrorism support or activities clearly identifies how the law enforcement network is divided in terms of competencies:

- *When proactive Internet policing is conducted on a long term base, which is usually conducted by intelligence services, to detect and monitor the movement of Islamist websites. The likelihood of detection and identification of the website administration increases significantly.*

- *On the other hand, when Internet policing is conducted by Law enforcement agencies for the aim of reactive policing, the likelihood of detection and identification of the website administration decreases because the primary objective is to prevent the crime from continuing.*

3. Could you indicate the main difficulties of the law enforcement authorities in Member States and your own organisation if applicable, to survey those who disseminate terrorist propaganda and bomb-making and other terrorist expertise through the internet?

In case your organisation keeps relevant statistics or data, we would be extremely grateful if you could make them available.

The number of terrorism related websites that need to be monitored in relation to the potential threat to the European Union and its Member States is huge and the scope of languages covered by these websites includes many non European languages. ***The problem of efficient website evaluation and assessment through native speakers continues to be a major one.*** *Not only have the officers in charge to read the language of the website, but also to speak and to understand the hidden messages of the Islamist extremist terrorism subculture or the specific content the website is concerned with or intended to address.*

4. Could you indicate the main difficulties of law enforcement authorities in Member States and your own organisation if applicable, to prosecute those who disseminate terrorist propaganda and bomb-making and other terrorist expertise through the internet?

In case your organisation keeps relevant statistics or data, we would be extremely grateful if you could make them available.

The main problem of law enforcement to forward a case to be prosecuted in the court of law is the identification of those who are responsible for the website and its contents.

Because the Internet is virtual and impersonal, the responsible person(s) can hide behind the medium's anonymity. Therein harboured is the reasoning of the increasing use of the Internet being a platform for Islamist propaganda and indoctrination.

To overcome these difficulties, prevention and neutralization of Islamist indoctrination and propaganda should be a top priority *on the agenda of law enforcement agencies and security or intelligence services alike.* ***Reluctances to share information between both sides need to be reduced through joint operations.***

A way of fighting against anonymity: users should be required to identify themselves to the provider before going online, at least as far as European jurisdictions are concerned.

5. Which measures, either legislative or not, would in your view be preferable to overcome the difficulties you have indicated in your answers to questions 3 and 4 above? Please, kindly detail your answer.

Member States should be encouraged to combat the phenomenon in a consistent effort and to share the burden. The duplication of efforts and waste of scarce resources can no longer be accepted. *There is an urgent and absolute need to develop a common platform where all non sensitive material related to the use of the Internet for terrorism support and propaganda should be pooled and made available to all European Law enforcement agencies. This is what is intended by the German Presidency's "Check the Web" initiative. However such an ambitious project needs to be supported by the intelligence community and legal constraints related to data protection have to be considered.*

Furthermore, resources need to be distributed to develop systematic training with respect to awareness, phenomenon, expertise, language, research and assessment training of law enforcement and intelligence institutions officers.

Considering that a wide range of terrorism related websites are out of range of Member States legislation, there is a need for a common European Union approach towards foreign States *which, knowingly or not, are harbouring terrorism-related websites to have them establish or change their legislation.*

While the European Union maintains a list of proscribed terrorist organisations, consideration should be given to drafting a list of terrorism-related websites; *such a list should be classified and frequently updated, but it would at least provide an evaluation instrument at European Union level.*

6. Which measures, either legislative or not, would in your view be preferable to improve the ability of law enforcement authorities in Member States and your own organisation if applicable, to address the more general threat of the use of new technologies and especially of the internet for terrorist purposes? Please, kindly detail your answer.

As for Europol, ***the main constraints*** *in relation to being proactive in monitoring and disseminating information related to terrorist propaganda on the Internet are:*

1. Limitations imposed by the Europol Convention preventing proactive approach when related to private chat rooms or forums.

2. Extensive data protection regime related to personal data which hinders free storage and exchange of assessment of information gathered from the Internet.

7. Concerning the measures you have referred to in your answers to questions 5 and 6:

a Could you estimate their costs for law enforcement authorities in Member States and your own organisation if applicable, and the need of economic support of the latter?

b) Could you estimate their impact on internet users, and their compatibility with freedom of expression and the right to respect for private and family life as laid down in the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe?

c) Could you estimate their impact on the effectiveness of the fight of law enforcement authorities against terrorism?

a) The estimation of development costs of a common exchange ***platform needs an in-depth study, but it would be relatively low*** *and should be considered in relation with the benefit generated by avoiding duplication of work amongst law enforcement agencies in the Member States.*

b) ***The question of data protection regime and protection of privacy and family life*** *for known terrorist who post statements on the Internet calling for mass murder should be considered.*

8. What are your views on the need to enhance the technological and linguistic resources of law enforcement authorities in Member States and your own organisation if applicable, in order to improve their ability to monitor the use of the internet for terrorist purposes? Please, kindly detail your answer.

There is a need for cooperation between law enforcement agencies and the intelligence community within the European Union and with external partners. *The main topics to be developed would be:*

- *To exchange information to avoid duplication of work between agencies*
- *To develop a common platform such as the one foreseen with the German initiative "Check the web" and with the Europol counter-terrorist Handbook Project, to provide law enforcement with readily available material.*
- *To develop technical training to ensure that all Member States have a minimum capability in the field of monitoring and countering terrorist propaganda on the Internet.*
- *To provide training for linguists in the relevant languages, including the enhancement of their cultural knowledge and their understanding of the groups or individuals they are facing. Thus they would be able to better assess the material found on the Internet.*

9. What are your views on the need to strengthen the instruction and training of law enforcement authorities in Member States and your own organisation if applicable, on the use of new technologies and especially the internet for terrorist purposes in order to improve their

ability to respond to the new modus operandi of terrorists groups? Please, kindly detail your answer.

*In the field of communication, the **private sector is constantly developing** a number of new technologies. There is a need to monitor these future developments in order to be prepared when these technologies will be on the market. For this purpose, **a good cooperation between the concerned agencies and the private sector is required.** Information gathered should in turn be made available to all Member States to avoid discrepancies in their respective capabilities.*

10. Concerning the enhancement of technological and linguistic resources as well as the strengthening of instruction and training as referred to in questions 8 and 9 above:

a) Could you estimate their costs for law enforcement authorities in the Member States and your own organisation if applicable, and the need of economic support of the latter?

b) Could you estimate their impact on the effectiveness of the fight of law authorities against terrorism?

It is not possible to assess the cost or impact of these measures without a proper study.

ANNEX IV: INSUFFICIENCY OF EU AND NATIONAL LEGISLATION APPLICABLE TO THE DISSEMINATION OF TERRORIST PROPAGANDA AND TERRORIST EXPERTISE

Table of contents

1. The Framework Decision on combating terrorism

The question addressed in this Annex is whether the Framework Decision on combating terrorism covers the transmission of both terrorist propaganda and terrorist expertise, in particular through the Internet. It is easy to verify that neither "terrorist propaganda" nor "terrorist expertise" are explicitly referred to in the instrument referred to. Nevertheless, it is more complex to examine whether such forms of behaviour are in fact covered by some of its provisions. Articles 2 (offences relating to a terrorist group) and 4 (inciting, aiding or abetting, and attempting) should be examined in this respect.

1.1 Article 2

a. The provision in the Framework Decision

Article 2 of the Framework Decision reads as follows:

"Offences related to a terrorist group,

1. For the purposes of this Framework Decision, "terrorist group" shall mean: a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences. "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

2. Each Member State shall take the necessary measures to ensure that the following intentional acts are punishable:

(a) directing a terrorist group;

(b) participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group."

It will therefore be examined whether the dissemination of terrorist propaganda and terrorist expertise fully or partially fit in "participating in the activities of a terrorist group with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group".

Two preliminary remarks can be made on Article 2(2) (b) before trying to answer the question above. Firstly, "supplying information or material resources, or by funding its activities in any way" constitute mere examples of a non exhaustive enumeration. Secondly, the "knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group" represents a compulsory requirement for any participation. Actually, this requirement comprises two requisites: not only must the participation contribute to the criminal activities of the terrorist group but the offender must also be aware of this.

For further clarification, The Commission Staff Working Paper annexed to the Report from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on combating terrorism (hereafter, the "report") provides for an interpretation of this provision on its page 14 reproduced below:

"From the Commission's point of view the rationale behind this provision is to provide for offences related to terrorist groups as independent criminal facts. Although this is not explicitly mentioned in the Framework Decision, it still derives from the logic of the instrument; as such offences they are specifically referred to in relation to inciting, aiding and abetting, have been assigned specific minimum-maximum penalties, may lead to the liability of legal persons or must be covered by rules on jurisdiction. Moreover the drafting of Article 2(2) (b) uses an extremely wide and open formula designed to embrace not only membership in a terrorist organisation but any other acts of assistance likely to contribute to the criminal activities of the group, even if undertaken by those who do not belong to or can not be proven to be members of the organisation. In addition this participation, as described in the Framework Decision, is not necessarily linked to the commission of specific terrorist offences, not even as concerns the intentional element. In this sense, the aim of Article 2(2) (b) is to ensure that those who through their actions, contribute to the development of a terrorist group may be prosecuted, even if such actions have no direct link with the commission of specific offences. To prevent an excessive incrimination, it is required that the offender acts with the knowledge that by his actions he will contribute, in general, to the criminal activities of the group. Should the intention to contribute to a specific offence be required, there would be no added value in relation to the general rules on criminal participation."

Despite this broad interpretation, it is doubtful that public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism through the internet are covered by Article 2(2) (b). Such propaganda aims at increasing the number of either supporters or violent activists but it is not linked to a particular terrorist group. There are many examples of

this kind of activity[94] that must be explained in the context of an increasingly decentralised terrorist activity, favoured by the Internet[95]: the modern terrorist network and particularly that of the global Djihadist movement, has no hierarchy anymore. It consists of a sum of lightly structured cells, sometimes linked to the network, sometimes independent[96]. Only one part of radical websites spread information about a specific terrorist group; the rest are concerned with the general movement of Djihad[97].

Something different is the case of terrorist propaganda, when it aims at the recruitment of new members into a terrorist group as well as the financing of a terrorist group. The explicit mentioning of terrorism funding as a form of participation leads to the conclusion that those collecting such funding should, with more reason, be considered as participants. The same goes for recruitment: if membership is a crime those recruiting new members should be punished even more seriously. However, the transmission of messages of propaganda aiming at collecting funds or recruiting new members is not strictly the same as actual fund-raising or recruiting.

In order to consider that both types of messages referred to here are in fact covered by Article 2, it might be argued that they represent an attempt at fund-raising and recruitment. However, Article 4 on inciting, aiding or abetting and attempting does not oblige Member States to ensure that attempting to commit an offence referred to in Article 2 is made punishable.

As for the transmission of terrorist expertise, we should highlight, firstly, that Article 2(2) (b) refers explicitly to "supplying information" as a way to participate in the activities of a terrorist group, which seems to suit perfectly the transmission of terrorism expertise. However, the requirement of contributing to the criminal activities of a terrorist group provides for a major threshold. In this sense, the transmission of expertise to an undetermined audience, such as online manuals posted in websites or chat-forums falls outside of the scope of Article 2(2) (b). And the same would apply to instructions addressed to specific potential recruits who, although they might be determined, by definition are not yet members of a terrorist group. This interpretation rules out a significant part of the transmission of terrorist expertise from the scope of application of Article 2. Furthermore, since the information supplied must "contribute to the terrorist activities of a terrorist group", it could be argued that terrorist expertise addressed to the members of a terrorist group but not useful for the criminal activities of that particular group would not be covered.

However, the dissemination of terrorist expertise to an undetermined audience or potential recruits may be punished a posteriori, if such information was actually accessed by the members of a terrorist group or the potential recruit joins a terrorist group and, in both cases, the said information contributes to the activities of the group.

It seems that a significant part of the dissemination of terrorist propaganda and terrorist expertise, amounting to public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism, is – as such - not punishable under Article 2. However, the dissemination of terrorist propaganda may be punished a posteriori, insofar as recipients are actually recruited into a terrorist group or provide for funding for a

94 See, i.e. "The use of the Internet by Islamic extremists", mentioned above, pp. 9 and 11.

95 See "Terrorist use of the Internet and fighting back", mentioned above, p. 11.

96 See "L'usage d'Internet à des fins terrorists", mentioned above, p. 5.

97 See "Jihadism online – A study of how Al-Quida and radical Islamist groups use the Internet for terrorist purposes", mentioned above, p. 15.

terrorist group. The dissemination of terrorist expertise is punishable as long as it is addressed to the members of a terrorist group and contributes to their criminal activities. The dissemination of terrorist expertise addressed to undetermined audience or to potential recruits may also be punishable a posteriori, if such information was accessed by the members of a terrorist group and contributes to its criminal activities.

b. National provisions implementing Article 2

First of all, the assessment of the first evaluation report should be examined[98]. Although it does not explore this question in particular, it analyses the content and scope of the different national provisions, which is useful for our purposes.

Some of the national provisions examined in the first evaluation report seem to have a broader scope than that of Article 2(2) (b). Germany and Portugal incriminate the "support" for respectively terrorist organisations and groups. However, Germany does not define the term and Portugal limits itself to reproduce the examples of participation of the Framework Decision. Germany, in addition, punishes those who recruit for a terrorist group. The United Kingdom punishes "inviting support" for proscribed organisation besides “belonging or professing to belong” to it while in Spain performing, requesting or facilitating any act of collaboration with the activities or purposes of a terrorist group constitutes an offence. In Austria, participation in a terrorist group consists of “taking part in its activities by supplying information or assets or in some other way in the knowledge that, by doing so, he is furthering the group or its offences”. Ireland incriminates the provision of assistance to a terrorist group. Finally, Italy and France condemn the participation in a terrorist group, using the terminology of Article 2, but they do not define it or include the requirement of “knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group”, which might also amount to a broader scope[99].

Concerning the information submitted in view of the second evaluation report, which is currently under elaboration, Member States already evaluated in the previous report have not forwarded new relevant provisions in this respect. However, the implementing provisions submitted by the Member States not yet evaluated constitute relevant information. Some of them seem to have a broader scope than that of Article 2(2) (b). For example, Luxembourg legislation punishes those that consciously and willingly participate actively in a terrorist group as well as those participating in the preparation or commission of a licit activity by a terrorist group, knowing that their participation will contribute to its objectives. Cyprus incriminates not only “involvement” in a terrorist group but also “support”, which is very broadly defined, covering both providing services and offering to provide them. Slovenian criminal code makes the participation in the activities of a criminal association punishable, irrespective of the actual commission of the criminal offences, without defining “participation”. In addition, other Member States incriminate membership or participation without defining it or including the requirement of Article 2, as it is the case of the Netherlands or Poland, which may also amount to a broader scope.

---

98 See Report from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on combating terrorism COM(2004) 409, as well as The Commission Staff Working Paper annex to the Report from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on combating terrorism, SEC(2004) 688.

99 See The Commission Staff Working Paper annex to the Report from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on combating terrorism, pp. 10-13.

Without prejudice to the relevant national case-law, not examined for the elaboration of the evaluation reports, it seems that various Member States have implemented Article 2 through provisions that cover the dissemination of terrorist propaganda to a further extent than this Article requires. In particular, some Member States have eliminated the requirement of contributing to the criminal activities of the terrorist group included in Article 2; others have changed it into a broader formula such as the Austrian "in the knowledge that, by doing so, he is furthering the group or its offences" or have included clarifications such as the Slovenian "irrespective of the actual commission of criminal offences". The use of terms such as "support" or "inviting support" suits even better the transmission of terrorist propaganda aiming at fund-rising or recruitment. Moreover, most Member States implement Article 4 through generally applicable provisions. As a consequence, attempting offences related to terrorist groups and, in particular, attempting to recruit members or to rise funding for a terrorist group would be punishable.

However, most of these national formulas seem to be still limited to propaganda referring to a terrorist group and resemble Article 2 in the sense that they would not cover messages intending to gain supporters for the terrorist cause or encourage supporters to engage into terrorist activity without referring to any terrorist group in particular.

By contrast with the transmission of terrorist propaganda, the national provisions implementing Article 2 do not seem to imply any significant advance in tackling the dissemination of terrorist expertise. Taking into consideration that the Framework Decision already refers to "supplying information" as a way of participation, broader formulas do not suit better the relevant behaviour. As for the main limit of Article 2 to cover the transmission of terrorist expertise, i.e. contributing to the criminal activities of a terrorist group, the situation remains unchanged under national implementing provisions.

National provisions implementing Article 2 of the Framework Decision generally seem to cover the dissemination of terrorist propaganda to a further extent than this Article requires. However, general publicity not linked to a specific terrorist group appears to remain uncovered by the relevant provisions in most Member States. The dissemination of terrorist expertise does not seem better tackled by Member States' implementing provisions than by Article 2 of the Framework Decision.

1.2 Article 4

a. The provision in the Framework Decision

Article 4 of the Framework Decision reads as follows:

"Inciting, aiding or abetting, and attempting

1. Each Member State shall take the necessary measures to ensure that inciting or aiding or abetting an offence referred to in Article 1(1), Articles 2 or 3 is made punishable.

2. Each Member State shall take the necessary measures to ensure that attempting to commit an offence referred to in Article 1(1) and Article 3, with the exception of possession as provided for in Article 1(1)(f) and the offence referred to in Article 1(1)(i), is made punishable."

The question to answer in this case is: does the obligation for Member States to "take the necessary measures to ensure that inciting or aiding or abetting an offence referred to in Article 1(1), Articles 2 or 3 is made punishable" cover, either fully or partially, the dissemination of terrorist propaganda or terrorist expertise?

Some preliminary remarks can be made. First of all, it is important to note that Article 4 refers to inciting, aiding or abetting not only the terrorist offences laid down in Article 1(1) of the Framework Decision but also to the offences relating to a terrorist group and offences linked to terrorist activities under Articles 2 and 3 of the same instrument. The combination of Articles 2 and 4 may be especially far reaching. For example, since funding the activities of a terrorist group constitutes a category of participation under Article 2, inciting, aiding or abetting the funding of terrorist activities falls within the scope of Article 4. And the same logic applies to the request for all kinds of participation in the activities a terrorist group, including invitations to become a member. It cannot be stated, however, that all messages requesting funding or new recruits for a terrorist group are automatically included in the scope of the provision in question. It is necessary to study the nature of inciting, aiding or abetting and see, in particular, whether messages that are not addressed to particular recipients but accessible to anyone in a website or restricted to “members” of a chat forum fit in the concept of participation.

Secondly, it must be stressed that Article 4 does not constitute an autonomous offence: inciting, aiding or abetting and attempting are only punished insofar as they are linked to other offences included in the Framework Decision. In particular, Member States are obliged to “ensure that inciting, aiding or abetting an offence referred to in Article 1(1), Articles 2 or 3 is made punishable”.

A strict interpretation of the required link to one of these offences would rule out the application of Article 4 to several messages of terrorist propaganda: for example, those that glorify suicide-bombers, justify terrorism or generally encourage to join the Djihad. Nevertheless, even under a broader interpretation, terrorist propaganda aiming at fund-raising or recruiting cannot be considered automatically covered by Article 4. As explained above, it will be necessary to study the nature of inciting, aiding or abetting and see whether messages that are not addressed to particular recipients respond to the concept of participation. In addition, it must also be considered whether messages that do not detail the circumstances of the offence, such as general calls for terrorist violence, can be qualified as participation.

As regards messages containing terrorist expertise, they might be easily considered to be forms of aiding or abetting under Article 4. But once more, an examination of whether “inciting, aiding or abetting” a criminal offence implies other requirements, in particular concerning the individualisation of the recipient as well as certain degree of determination of the circumstances of the offence is still required.

Finally, Article 4 does not require Member States to ensure that attempting to incite, aide or abet is made punishable. This is because Article 4(2) only obliges Member States to incriminate the attempt of the offences laid down by Articles 1(1) and 3. Following this reasoning, messages posted on the Internet would be excluded from the scope of Article 4 unless a recipient was actually incited, aided or abetted to commit one of the relevant offences. Under this interpretation, the Framework Decision would not require that the transmission of terrorism propaganda or terrorist expertise itself is made punishable. So, even if the message was addressed to a particular person and represented a clear intent of inciting,

aiding or abetting the commission of a circumstanced offence, its author would not be punishable under Article 4 unless the recipient was actually incited, aided or abetted.

It is doubtful that the dissemination of terrorist propaganda or terrorist expertise itself is not punishable under Article 4, since the mere attempt of incitement, aide or abet is not incriminated. This behaviour may be incriminated *a posteriori* insofar if specific recipients are actually incited, aided or abetted to commit some of the offences referred to in Articles 1(1), 2 and 3.

b. Doctrinal background: authorship and participation in comparative law

In order to better understand both Article 4 and the national provisions on participation and common commission of offences, a brief explanation of the main doctrinal positions is offered under this section. The commission of an offence together with others receives very different treatments under the various national systems stemming from two main concepts of complicity: the theory of the plurality of offences, for which there are as many offences as co-operators and the theory of the unity of the offence, for which several persons co-operate to the commission of a single offence.

The plurality of offences implies that every co-operator shall be punished for his own offence and any distinction between perpetrator, accomplice, instigator or other becomes irrelevant. Furthermore, it implies that the aggravating circumstances between the co-operators are not transferable.

The unity of the offence, on the other hand, assumes that the co-operators do not necessarily have the same role and creates different categories, mainly that of the accomplice. The criminality of his act “derives” from the criminality of the act committed by the main perpetrator.

The unity of the offence is the dominant theory, followed by most criminal laws[100]. However, it comprises different systems, depending on the categories used: some only distinguish between the main author and the accomplice or accessory, some add the concept of “accomplice after the fact” or “receleur”, some use the category of “instigator”, some national systems make a distinction between direct and indirect accomplices.... Despite the divergences, some common rules may be established: every form of complicity requires the intent of the agent and the action of the accomplice has to be linked to the main action.

Among the legal systems following the dominant theory, in some of them incitement is not punishable unless the offence is committed, or at least the commission has started, whereas in others incitement is punishable even in the absence of any result. The common law falls in this last group, punishing incitement as an autonomous offence. According to the example of the English case law, a material and intentional elements are required: the behaviour, which is very broadly described as the fact of “persuading, asking, corrupting, threatening, and this either explicitly or implicitly” and “the intention of the instigator that the offence will be

100 The article "Grunderfordernisse einer Regelung des Allgemeinen Teils", in "Wirtschaftsstrafrecht in der Europäischen Union", (Rechtsdogmatik- Rechtsvergleich-Rechtspolitik), Freiburg-Symposium, Tiedemann (ed.), Carl Heymanns Verlag KG. München, 2001, identifies Austria, Italy, Denmark and Norway as criminal codes adopting the theory of the plurality of offences and notes that all other Members of the European Union follow the theory of the unity of the offence. The article, however, precedes the enlargement of 1 May 2004.

committed, which implies the knowledge of all circumstances of this offence, including the intention of the perpetrator(...)"[101].

Concerning the theory of the plurality, anybody materialising an element required for the commission of the offence is considered a perpetrator, his behaviour being punishable according to his intention. As a consequence, the co-operator is criminally liable irrespective of the liability of the rest of co-perpetrators and whether or not they have come to the commission or the attempt of an offence. Moreover, under this model, attempted participation is punishable. However, it cannot be excluded that the criminal liability of the participant requires certain degree of determination of the circumstances of the final offence or the individualisation of the co-perpetrators.

It can be defended that under the theory of the unity of the offence, participation requires either the commission of the offence, its attempt, or at least a concrete idea or project of the commission of a specific offence. Furthermore, it seems that the perpetrator or potential perpetrator needs to be individualised, either because he commits or attempts to commit the offence or because the participant knows his intention. Under the theory of the plurality, participation does not seem to require the commission or attempt of the final offence. It remains uncertain whether the criminal liability of the participant requires certain degree of determination of the circumstances of the final offence and the identity of the co-authors.

The aim of this section is not to classify Member States under one of the two theories and extract the conclusions from this sole basis. However, this background constitutes a relevant reference: offering a general idea of these opposed concepts may be important to better understand the national provisions on participation and common commission of offences that will be explained below.

c. National provisions implementing Article 4

First of all, we will examine the assessment of the first evaluation report[102]. While going through the analysis of the different national provisions, two Member States stand out: Ireland and Spain. Ireland not only provides generally that any person who aids, abets, counsels or procures the commission of an indictable offence is liable to be indicted, tried and punished as a principal offender, but also makes it an offence for any person to recruit, incite or invite another person – or other persons generally - to join an unlawful organisation or to take part in, support or assist in its activities. Spain criminalises provocation in addition to instigation. Provocation is defined as public instigation and only applies if the offence is not committed.

But, although it is interesting to note the existence of such "parallel" provisions, the report does not provide for any hint of the wider or narrower scope of inciting, aiding or abetting under the national provisions. The table annex to the report contains however relevant information, very often directing the reader to general provisions on participation. The study of the general provisions on participation together with the examination of additional provisions submitted by some Member States in view of the elaboration of the second

---

101 See "Droit pénal comparé spécial, Dalloz, 2002, mentioned above, pp. 312-325.

102 See The Commission Staff Working Paper annex to the Report from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on combating terrorism, pp. 18-19.

evaluation report, has led to some interesting findings irrespective of the national case-law, which, as explained above, is not examined for the elaboration of the reports.

National provisions from an important number of Member States explicitly require participation to be intentional (Finland, France, Germany, Latvia, Lithuania, Portugal and Slovenia) while only Sweden foresees the possibility of negligent participation. Since the concepts of transmission of terrorist propaganda and terrorist expertise require the intent of the author, national provisions would cover it in both cases.

For some Member States, participation is made punishable only when the offence has been started or attempted (as Portugal, Slovak Republic and Spain clarify). Such requirement limits the scope of participation. Other Member States go beyond the level required by the Framework Decision by making the attempt of incitement punishable: for example Italy in Article 302 of its penal code, punishing certain intentional serious crimes, amongst them certain terrorist offences, when incitement is not followed by an agreement or by the commission of the offence; Poland, making the attempt of incitement explicitly punishable in Article 18 of its criminal code and similarly Germany in Article 30 of its penal code. Sweden not only makes attempted incitement punishable but also attempted complicity in Chapter 23 of its penal code. Similarly, Austria generally incriminates attempted perpetration and participation under Article 15(3) of its penal code. Finland also goes beyond the Framework Decision, although in another direction, by making instigation to participation punishable.

It should also be noted that Article 115 of the Italian penal code incriminates the agreement of the co-operators to commit the offence, even if finally it is not committed. Under Articles 21 and 23 of the Danish penal code it is clear that the participant is punished even if the offence is not carried out, and Article 26 of the Slovenian penal code explains that solicitation is punished even if the offence is not attempted. Similarly, Latvian penal code clarifies that, if the perpetrator does not start the execution of the offence, the joint participants will be liable for preparation of the offence in question.

Even if some Member States make the attempt to incite or participate punishable, it does not mean necessarily that they cover most of the cases of dissemination of terrorist propaganda and terrorist expertise through the Internet. Cases of transmission to a specific recipient, addressed as a possible main perpetrator of a defined offence will normally be covered. However, it is doubtful that such national rules cover the cases that represent an important part of this report: messages disseminated through a website or a chat-forum, where the main author and circumstances of the eventual offence are not determined.

Finally, national provisions on public incitement, provocation or dissemination of propaganda of a general nature should be examined. The analysis of the table annexed to the report together with the additional information sent in view of the elaboration of the second report reveal that not only Ireland and Spain have adopted this kind of provisions. For example, the Belgian penal code refers explicitly to the case of "public provocation" under Article 66, punishable even if the offence is not perpetrated. Section 164 of the Slovak penal code criminalises "public incitement". France refers to Articles 23 and 24 of the Law on the Freedom of the Press of 29 July 1881 which refers to direct provocation to commit terrorist offences or their apology through the press, the distribution of printed documents or drawings as well as their exhibition in public places and their distribution, including via e-communications, as well as through speeches or threats pronounced in public places. Finally the Cypriot Bill Section 6 makes the possession of documents with seditious content punishable and publication etc. of propaganda material of an unlawful organisation qualifies

as a terrorist offence. Germany adopted Article 129a, paragraph 5, of its Criminal Code dealing with recruitment or propaganda in favour of a terrorist group.

Some of these provisions specify that the perpetration of the offence is not required for the behaviour to be punishable. The common point in all these provisions is that they punish publishing a message addressed to a large audience. They therefore appear to cover the dissemination of terrorist propaganda and terrorist expertise through the Internet, even if the propaganda or expertise is accessible to anyone on a website.

The variety of national rules on participation and common commission of offences, together with the existence of additional provisions which look very much the same as the former, with the difference that a message is addressed to a wide audience, may seem chaotic. Nonetheless, the analysis of the answers to the questionnaire under Section 3.1 will reveal the logic lying behind. At this stage, only the following conclusions can be formulated:

Some Member States go beyond the Framework Decision by making the attempt to incite punishable. It is however doubtful that such national rules cover the dissemination of terrorist propaganda and terrorist expertise through a website or a chat-forum, where the main perpetrator and circumstances of the eventual offence are not determined. It seems that, in order to punish this behaviour under national law, national conceptions of participation and incitement should not require that the eventual perpetrator and the circumstances of the eventual offence are determined at the moment of the incitement or the participation.

1.3. Additional national legislation

In the consultation process referred to in Section 1, Member States were asked about national provisions, in addition to those implementing the Framework Decision, that may apply to transmission of terrorist propaganda and terrorist expertise through the media and the internet in particular[103]. Two Member States did not provide for any answer or answered very briefly because of their undergoing legislative modification in view of the ratification of the Convention on the Prevention of Terrorism of the Council of Europe[104]. The rest of the Member States save one included different provisions to those submitted in view of the elaboration of the evaluation reports[105]. Yet many combined these different provisions or envisaged provisions with some already analysed under the evaluation reports. As we have already commented on national provisions implementing the Framework Decision, the focus of this paragraph will be the complementary information provided for by Member States[106].

A first overview shows that every Member State but one have got or will have specific rules dealing with public dissemination of messages encouraging the commission of terrorist offences (and often of other crimes). Although terminology is not at all uniform (i.e. "provocation", "instigation", "public incitement" etc.) we observe that there is a reiterative

---

103 See the questionnaire addressed to Member States in view of the eventual revision of the Framework Decision on combating terrorism and the compilation of their answers in Annex I.

104 The Convention on the Prevention of Terrorism will be analysed under a section dealing with International instruments applicable to the dissemination of terrorist propaganda and terrorist expertise.

105 It must be noted that some Member States answering the questionnaire were not evaluated in the first report nor did they submit the information in view of the elaboration of the second report. This is the case of Greece and, for obvious reasons, of Bulgaria and Romania, since the cut-off date taken to admit information on national implementation was 31 July 2006.

106 For the full analysis of the answers from Member States, see Annex I.

characteristic: they explicitly refer to publicly disseminated information. Often, the provision makes reference to oral dissemination in a meeting, via written publications or audiovisual material. Some provisions deal specifically with "terrorist publications", including even a reference to dissemination via the Internet. In other cases, the comments of the Member States explain that messages on the internet are included. Two Member States express this characteristic theoretically by saying that the recipient does not have to be previously determined. Actually, these two Member States stress that, by contrast with the general rules on incitement, in the relevant provisions the offence does not need to be determined beforehand either. In this sense, some Member States retain direct and indirect provocation. In five Member States, these provisions refer to the irrelevance of the subsequent commission of the offence or the actual incitement of the recipients of the message.

Additionally, eight Member States have got or will have provisions condemning glorification or approval of terrorist offences (and often of other crimes).

Two Member States deal specifically with the denigration or humiliation of the victims. Two also refer to apology of terrorism or crime apology.

Three Member States referred to provisions explicitly covering the public dissemination of terrorist expertise. Six Member States have got or will have provisions on training or recruiting, mainly resulting from the adaptation of their legislation to the Council of Europe Convention on the Prevention of Terrorism. One Member State refers to its provision on preparation of a crime, explaining that it comprises holding something especially intended to be used as an auxiliary means and that compiled information can be regarded as the said auxiliary means. In this case the intent does not have to cover a specific terrorist offence. Another Member State refers to its general rules on complicity. Three Member States explain that the transmission of terrorist expertise is criminalised under the penal code only if done intentionally and the terrorist act was actually committed or attempted/planned. Two Member State link the dissemination of terrorist expertise to terrorist groups, making the transmission information on terrorist targets punishable. One Member State clarifies that it has no specific provisions concerning the transmission of terrorism expertise in place.

1.4 Conclusions

1. It is doubtful that Article 4 of the Framework Decision requires Member States to ensure that the dissemination of messages through the Internet encouraging the commission of terrorist offences, either accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment, is made punishable.

As stated above, Article 4 does not include the obligation for Member States to ensure that attempts to incite others to commit terrorist offences are made punishable. Following this reasoning, the provision only obliges Member States to incriminate incitement when at least one of the recipients of the message is actually incited. Under this interpretation, Article 4 does not require Member States to make the dissemination of messages encouraging the commission of terrorist offences via the Internet itself punishable.

Furthermore, concerning public dissemination (the case of messages accessible to anyone), the first evaluation report on the national implementation of Article 4 concluded that all Member States would be able to meet the terms of Article 4 through their national provisions on complicity and inchoate offences whereas only three Member States had submitted

provisions dealing with public dissemination of messages encouraging the commission of terrorist offences.

2. It is doubtful that Article 4 of the Framework Decision requires Member States to ensure that the dissemination of messages through the Internet providing for terrorist expertise, either accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment, is made punishable.

This provision does not require Member States to ensure that the attempt of aiding or abetting others to commit terrorist offences is made punishable and it seems that the dissemination of the messages referred to above via the Internet should be qualified as an attempt.

3. It seems that Article 2 of the Framework Decision does not require Member States to ensure that a significant part of the dissemination of messages through the Internet encouraging the commission of terrorist offences, either accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment is made punishable.

Article 2 includes the requirement of contributing to the criminal activities of a terrorist group. In this sense, it could be defended that messages accessible to anyone, restricted to members of a chat-forum or addressed to potential recruits fall out of the scope of Article 2. Concerning messages aimed at fund-raising or recruitment for a terrorist group, they seem to meet such requirement. However, these messages would actually constitute an attempt of fund-raising and recruitment and the criminalisation of attempt under Article 4 does not cover the attempt to commit offences related to terrorist groups.

4. It seems that Article 2 of the Framework Decision does not require Member States to ensure that a significant part of the dissemination of messages through the Internet providing for terrorist expertise, either accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment is made punishable, save in exceptional cases.

Once again, since Article 2 includes the requirement of contributing to the criminal activities of a terrorist group. It could be argued that the dissemination of terrorist expertise is not covered by Article 2 insofar as the recipients are undetermined (i.e. messages accessible to anyone or disseminated in a chat forum) or potential recruits.

6. Most Member States that replied to the questionnaire have got provisions addressing direct invitations to commit a specific terrorist offence through messages accessible to anyone (i.e. website), restricted (i.e. chat forum) and addressed to pre-selected candidates for recruitment.

Nevertheless, it is doubtful that many would cover general encouragement to join the Djihad, without reference to a specific terrorist offence. However, the offences on recruitment introduced by some Member States may cover such messages, at least when they are addressed to pre-selected candidates. These messages, when associated to the name of a certain terrorist group, are likely to be covered by the legislation of many Member States. Indeed, as it has been explained above, numerous Member States have got far-reaching provisions that implement Article 2 and might apply to the propaganda in favour of a terrorist group.

7. Few Member States have provisions that explicitly cover the transmission of terrorism expertise which are applicable to either messages accessible to anyone (i.e. website), restricted (i.e. chat forum) or addressed to pre-selected candidates for recruitment.

Sweden, through very far reaching concepts of preparation and participation in an offence, would at least cover the dissemination of expertise to pre-selected candidates and the same goes for the offences introduced by some Member States on training and instruction, mainly adopted in view of the ratification of the Council of Europe Convention on the Prevention of Terrorism.

8. Generally speaking, national provisions of Member States, although not harmonised, substantially cover the dissemination of terrorist propaganda and in some cases also terrorist expertise while the Framework Decision on combating terrorism seems to stay behind. Furthermore, the European instrument already appears to be out-dated in the international context, where the Council of Europe[107] and the United Nations[108] have set the basis for further reaching national legislation.

2. Other instruments: The Television without frontiers Directive[109], the Directive on electronic commerce[110] and the Data retention Directive[111].

The Television without frontiers Directive aims to ensure the free movement of broadcasting services within the internal market and at the same time to preserve certain public interest objectives, such as cultural diversity, the right of reply, consumer protection and the protection of minors. It is also intended to promote the distribution and production of European audiovisual programmes, for example by ensuring that they are given a majority position in television channels' programme schedules.

The Directive prohibits incitement to hatred on grounds of race, sex, religion or nationality in broadcast. This includes third country programmes (mostly satellite television) if they use either a frequency, satellite capacity or an uplink appertaining to a Member State. Member States are responsible for the implementation of these rules and, as noted in the Communication on Radicalisation and Recruitment, cases of prohibition to retransmit channels like al-Manar or Sahar-1 within Europe show that the effective application of these rules works quite well.

---

107 See the Council of Europe Convention on the Prevention of Terrorism, mentioned above.

108 The Report of the Secretary-General of the United Nations "Uniting against terrorism: recommendations for a global counter-terrorism strategy", interprets Security Council Resolution 1624 (2005) as providing for a basis for the criminalization of incitement to terrorist acts and recruitment, including through the Internet.

109 Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (OJ L 202, 30.7.1997, p. 60).

110 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

111 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

The Directive was amended in 1997 for the first time. In December 2005, the Commission published a proposal for revision of the Directive, aimed at modernising the existing rules, which is still under discussion in the Parliament and the Council.

Additionally, it should be noted that the revision of the Directive underway would broaden its scope so that the instrument would cover certain content transmitted through the Internet. The Directive would apply to the delivery of moving images with or without sound, in order to inform, entertain or educate, to the general public, also when transmitted by electronic communication networks provided that the audiovisual content is not merely incidental to the service but its principal purpose.

It seems that messages disseminating terrorist propaganda and terrorist expertise will be, at least in some cases, covered by the prohibition of incitement to hatred. Therefore, the prohibition of the television without frontiers would apply to the content under examination. Nevertheless, the Directive will not be applicable to all content disseminated via the Internet even after its revision nor, obviously, does it allow for the prosecution of the person responsible for the dissemination of terrorist propaganda and terrorist expertise.

The Directive on electronic commerce seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States. To this end, it approximates certain national provisions, including rules on the liability of intermediaries.

In particular, under Article 12, service providers are broadly exempted from liability regarding the information they transmit or give access to ("mere conduit"). Articles 13 and 14 deal, respectively, with their liability as intermediates that automatically and temporarily store information ("caching") or that store it at the request of the recipient of the service ("hosting"). In these cases, they are not liable unless they have actual knowledge of the illegal activity or information. Such exemptions, though, do not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, including the removal of illegal information or the disabling of access to it.

Additionally, Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store or a general obligation actively to seek facts or circumstances indicating illegal activity. Nonetheless, the provision states that Member States may establish obligations for service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

This liability regime is important from the point of view of the fight against terrorism. Firstly, it allows for co-operation with law enforcement authorities so that Member States can require service providers to provide law enforcement authorities with certain data which might be of utmost importance in the investigation of terrorist cases. Furthermore, this regime allows for "notice and take down" procedures, by which the service providers storing illegal content can become liable when they do not remove illegal information after they are given notice of its presence. In order to be able to benefit from this liability regime as regards the dissemination of terrorist propaganda and terrorist expertise through the Internet is qualifying this behaviour as illegal. Its application does not require that the behaviour is made punishable. Forbidding

the dissemination of terrorist propaganda and terrorist expertise suffices. So, even if the dissemination of terrorist propaganda and terrorist expertise is not incriminated, the liability regime would apply if non-criminal law in Member States forbids this behaviour. Few Member States, however, seem to have relevant legislation in this sense[112]. Once again, even if the Directive on electronic commerce applies, it obviously does not allow for the prosecution of the responsible behind the dissemination of terrorist propaganda and terrorist expertise.

The Directive on data retention aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. It is important to note that this instrument does not apply to the content of electronic communications, including information consulted using an electronic communications network. It applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user.

If the dissemination of terrorist propaganda and terrorist expertise through the Internet were qualified as serious crimes, public authorities could be assisted in the detection, investigation and prosecution of these forms of behaviour by the providers referred to above, to which they could request traffic and location data, crucial to identify the responsible individuals behind such dissemination.

Therefore, it can be concluded that:

1. **The Television without frontiers Directive** does not currently apply to the Internet and after its ongoing revision will only apply to a restricted portion of its content. In addition, it does not directly outlaw the dissemination of terrorist propaganda and terrorist expertise but prohibits incitement to hatred. It follows that this instrument provides for a rather limited solution to tackle the dissemination of terrorist propaganda and terrorist expertise, especially through the Internet.

2. **The Directive on electronic commerce** allows law enforcement authorities to request internet service providers to remove content from or disable access to a website. However, its application requires that the dissemination of terrorist propaganda or terrorist expertise is outlawed. In many Member States the dissemination of terrorist propaganda or terrorist expertise is not fully incriminated or forbidden, excluding the use of the co-operation channels foreseen under the e commerce.

3. **The Data retention Directive** allows law enforcement authorities to request internet service providers to provide location and traffic data. Nevertheless, the data retention Directive only applies to serious crimes. It follows that the partial lack of incrimination of the dissemination of terrorist propaganda and terrorist expertise by many Member States excludes the request of data from service providers in the field of criminal law.

112 See Annex I.

RAT DER EUROPÄISCHEN UNION

Brüssel, den 13. November 2007 (14.11)
(OR. en)

Interinstitutionelles Dossier:
2007/0236 (CNS)

14960/07
ADD 2

CATS 122
DROIPEN 104

ADDENDUM ZUM VORSCHLAG

der:	Europäischen Kommission
vom:	12. November 2007
Betr.:	ARBEITSDOKUMENT DER KOMMISSIONSDIENSTSTELLEN Begleitdokument zum Vorschlag für einen RAHMENBESCHLUSS DES RATES zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Die Delegationen erhalten in der Anlage den mit Schreiben von Herrn Jordi AYET PUIGARNAU, Direktor, an den Generalsekretär/Hohen Vertreter, Herrn Javier SOLANA, übermittelten Vorschlag der Europäischen Kommission.

Anl.: SEK(2007) 1425

KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 6.11.2007
SEK(2007) 1425

ARBEITSDOKUMENT DER KOMMISSIONSDIENSTSTELLEN

Begleitdokument zum

Vorschlag für einen

Rahmenbeschluss des Rates zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

{KOM(2007) 650 endgültig}
{SEK(2007) 1424}

Zusammenfassung der Folgenabschätzung

TEIL 1: VERFAHREN UND KONSULTATION DER BETEILIGTEN KREISE

Das Legislativ- und Arbeitsprogramm der Kommission für 2007 enthält einen Vorschlag für eine Änderung des Rahmenbeschlusses des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (nachstehend der „Rahmenbeschluss“). Ziel dieser Änderung ist es, der Verbreitung terroristischer Propaganda über die Medien entgegenzuwirken und die Weitergabe von terroristischem Wissen, insbesondere über den Umgang mit Sprengstoffen und den Bau von Bomben für terroristische Zwecke, zu beschränken.

Im Juni 2006 wurde eine umfassende Bestandsaufnahme durchgeführt, in deren Rahmen die Kommission drei verschiedene Fragebögen versandte: einen an die Mitgliedstaaten (26. Juni 2006), einen an die Medien, die Wirtschaft und die Zivilgesellschaft (20. November 2006) und einen weiteren an Europol und Eurojust (11. Dezember 2006). Eine Zusammenfassung der Antworten auf die Fragebögen ist in den Anhängen I, II und III zu der Folgenabschätzung nachzulesen. Darüber hinaus fanden Gespräche und Zusammenkünfte mit Vertretern der europäischen Medien und Internetanbieter statt. Am 20. März 2007 schließlich kamen auf einer Konferenz Vertreter der Mitgliedstaaten, von Europol sowie Eurojust und Cepol zusammen, um die Ergebnisse aus den Fragebögen zu erörtern und sich Gedanken darüber zu machen, wie der Missbrauch des Internets für terroristische Zwecke unterbunden werden kann.

TEIL 2: PROBLEMATIK

Moderne Informations- und Kommunikationstechnologien spielen bei der Ausbreitung der terroristischen Bedrohung eine erhebliche Rolle. Insbesondere das Internet ist ein preiswertes, schnelles, leicht zugängliches Medium mit praktisch globaler Reichweite. All diese Vorteile, die gesetzestreue Bürger, die das Internet tagtäglich nutzen, sehr zu schätzen wissen, machen sich auch Terroristen zunutze, die das Potenzial des Internet voll erkannt haben: Sie nutzen dieses grenzenlose Medium sowohl für die Verbreitung ihrer Propaganda, um Anhänger zu gewinnen und zu mobilisieren, als auch für die Verbreitung von Anleitungen und Online-Handbüchern für die Terrorismus-Ausbildung oder die Planung von Terroranschlägen. Die damit verbundenen Kosten und Risiken sind äußerst gering.

Das Internet trägt auf diese Weise maßgeblich zur Verstärkung des Radikalisierungs- und Rekrutierungsprozesses bei: Es wird zur Beeinflussung und Mobilisierung von Einzelpersonen und lokalen Netzwerken in Europa eingesetzt und dient darüber hinaus als „virtuelles Trainingscamp“, indem es Informationen über Mittel und Methoden des Terrorismus verbreitet. Die Verbreitung terroristischer Propaganda und terroristischen Wissens über das Internet trägt dazu bei, den Kreis terroristischer Aktivisten zu festigen und so die terroristische Bedrohung zu verstärken. Angesichts der rasch wachsenden Zahl von Nutzern, durch die das Internet einen noch höheren Stellenwert in der modernen Gesellschaft haben wird, muss davon ausgegangen werden, dass die Verbreitung terroristischer Inhalte weiter zunehmen wird.

Für die Strafverfolgungsbehörden ist es schwer, die Spirale aus Radikalisierung und Terroranschlägen zu durchbrechen, die sich aus der terroristischen Propaganda und dem

terroristischen Wissen - insbesondere über das Internet - speist. Die Schwierigkeiten sind auf unzureichende Rechtsvorschriften zurückzuführen sowie auf fehlende Kapazitäten und mangelnde Kenntnis der zahlreichen Sprachen, in denen die terroristische Propaganda und das terroristische Wissen verbreitet werden, und nicht zuletzt auf die Beschaffenheit des Internets, das durch seine Extraterritorialität und Anonymität die Arbeit der Strafverfolgungsbehörden ernsthaft behindert und die Entfernung derartiger Inhalte aus dem Netz sowie die Aufdeckung und Strafverfolgung der für solche Webseiten und ihren Inhalt verantwortlichen Personen erschwert.

Die Prüfung der einzelstaatlichen Rechtsvorschriften hat gezeigt, dass die Verbreitung terroristischer Propaganda und terroristischen Wissens nicht in allen Mitgliedstaaten strafrechtlich verfolgt wird. Unzureichende Rechtsvorschriften in Bezug auf die Verbreitung von Anleitungen zum Bau von Bomben für terroristische Zwecke und sonstigem terroristischem Wissen sowie große Unterschiede zwischen den rechtlichen Mitteln der Mitgliedstaaten, insbesondere in Bezug auf die Verbreitung terroristischer Propaganda, zeigen, dass es in diesem Bereich eine Sicherheitslücke zu schließen und die entsprechenden Rechtsvorschriften anzugleichen gilt.

Die öffentliche Aufforderung zur Begehung einer terroristischen Straftat sowie die Anwerbung und Ausbildung für terroristische Zwecke sind im EU-Recht nicht explizit geregelt. Außerdem ist im Rahmenbeschluss zur Bekämpfung des Terrorismus nicht eindeutig festgelegt, dass die Mitgliedstaaten gewährleisten müssen, dass ein bedeutender Anteil der über das Internet verbreiteten Aufforderungen zur Begehung einer terroristischen Straftat oder zur Bereitstellung terroristischen Wissens, das für jedermann zugänglich ist (Website), das beschränkt zugänglich ist (Chat-Forum) oder das an einen ausgewählten Personenkreis gerichtet ist, unter Strafe gestellt wird.

Die Nutzung des Internets zur Verbreitung öffentlicher Aufforderungen zur Begehung terroristischer Straftaten sowie zur Anwerbung und Ausbildung für terroristische Zwecke ist allerdings Gegenstand des Übereinkommens des Europarats zur Verhütung des Terrorismus, das darüber hinaus Bedingungen und Garantien enthält, die die Achtung der Menschenrechte, insbesondere das Recht der freien Meinungsäußerung, gewährleisten. Das Übereinkommen wird zu einer Angleichung der Rechtsvorschriften der Mitgliedstaaten in diesem Bereich führen, wenn alle es unterzeichnet und ratifiziert haben.

Jede Regelung in diesem Bereich, die Fragen betrifft, die sich im Grenzbereich zwischen der rechtmäßigen Ausübung von Freiheitsrechten (wie der Meinungs-, Vereinigungs- oder Religionsfreiheit) und kriminellem Verhalten bewegen, wirkt sich zwangsläufig direkt auf die Grundrechte aus. Bei der Begründung eines neuen Straftatbestands und der Einführung entsprechender Straf- und Durchführungsbestimmungen muss den Grundrechten Rechnung getragen werden und damit auch dem Verhältnismäßigkeitsprinzip, wonach jede Maßnahme, die in Grundrechte eingreift, in einer demokratischen Gesellschaft einen legitimen öffentlichen Zweck verfolgen und erforderlich sein muss; jede Form willkürlicher, diskriminierender oder rassistischer Behandlung ist ausgeschlossen[1].

---

1 Siehe Erläuternder Bericht zum Übereinkommen des Europarats zur Verhütung des Terrorismus, Ziff. 143-151.

TEIL 3: ZIELE

Wirksame Maßnahmen zur Eindämmung von über das Internet verbreiteten Aufforderungen zur Begehung terroristischer Straftaten sowie zur Anwerbung und Ausbildung für terroristische Zwecke könnten verhindern helfen, dass sich eine stärkere und breitere Plattform für terroristische Aktivisten und Sympathisanten entwickelt. Derartige Maßnahmen sollten neben Rechtsvorschriften, mit denen die vorerwähnte Sicherheitslücke zu schließen ist, auch praxisbezogene Maßnahmen zur Stärkung der Kapazitäten und des Fachwissens der Strafverfolgungsbehörden umfassen. Mit diesen Maßnahmen ließe sich das Risiko terroristischer Anschläge verringern und die Möglichkeiten der Radikalisierung und Rekrutierung reduzieren.

Die Rechtsvorschriften sollten ganz eindeutig vorsehen, dass die Strafverfolgungsbehörden berechtigt sind, Ermittlungen wegen Verbreitung terroristischer Propaganda und terroristischen Wissens, auch über das Internet, zu führen und terroristische Aktivisten und Sympathisanten, die hinter derartigen Inhalten stecken, unionsweit zu verfolgen. Außerdem sollten die Strafverfolgungsbehörden die auf dem Gebiet der Terrorismusbekämpfung bereits erzielte Rechtsangleichung und die zur Verfügung stehenden Kooperationsinstrumente wie den Europäischen Haftbefehl beim Vorgehen gegen diese neuen Formen kriminellen Handelns anwenden dürfen.

Im Rahmen der praxisbezogenen Maßnahmen sollten geeignete Fortbildungsmaßnahmen und eine ausreichende materielle Ausstattung der Strafverfolgungsbehörden vorgesehen werden sowie eine qualifizierte Unterstützung durch IT-Fachleute und Experten mit Sprachkenntnissen, mit deren Hilfe Gewaltinhalte im Internet aufgespürt und analysiert und die Verantwortlichen, die hinter der Verbreitung solcher Inhalte stecken, identifiziert werden können.

TEIL 4: POLITISCHE OPTIONEN

Das angestrebte Ziel lässt sich durch folgende Optionen erreichen:

(1) Beibehaltung der bisherigen Politik. Die Beibehaltung des Status quo erscheint angesichts des Übereinkommens des Europarats zur Verhütung des Terrorismus und des laufenden Unterzeichnungs- und Ratifizierungsprozesses fragwürdig.

(2) Internetanbietern wird untersagt, Zugang zu Inhalten zu gewähren, die auf eine öffentliche Aufforderung zur Begehung einer terroristischen Straftat, Anwerbung oder Ausbildung für terroristische Zwecke gerichtet sind. Diese Option führt eine neue Verpflichtung ein, die für Diensteanbieter allgemein gilt, und ändert damit die E-Commerce-Richtlinie ganz beträchtlich.

(3) Die Strafverfolgungsbehörden werden in die Lage versetzt, sich mehr Kapazitäten und Fachkenntnisse anzueignen, mit denen sie dem Missbrauch des Internets für terroristische Zwecke entgegenwirken können. Diese Option sieht die Finanzierung geeigneter Schulungen, einer leistungsfähigen Ausrüstung und der Mitarbeit von Experten vor, damit die Strafverfolgungsbehörden Inhalte, die auf eine öffentliche Aufforderung zur Begehung einer terroristischen Straftat, Anwerbung oder Ausbildung für terroristische Zwecke gerichtet sind, schneller erkennen und

analysieren und die verantwortlichen terroristischen Aktivisten und Sympathisanten verfolgen können.

(4) Die Mitgliedstaaten werden nachdrücklich aufgefordert, das Übereinkommen des Europarats zur Verhütung des Terrorismus zu unterzeichnen bzw. zu ratifizieren. Bei dieser Option handelt es sich um eine politische Erklärung, durch die die Unterzeichnung und Ratifikation des Übereinkommens beschleunigt werden soll.

(5) Der Rahmenbeschluss zur Terrorismusbekämpfung wird geändert, um im Einklang mit dem Übereinkommen des Europarats zur Verhütung des Terrorismus Straftatbestände aufzunehmen, die die öffentliche Aufforderung zur Begehung einer terroristischen Straftat sowie die Anwerbung und Ausbildung für terroristische Zwecke, einschließlich über das Internet, unter Strafe stellen.

TEILE 5 UND 6: VERGLEICH UND FOLGEN DER OPTIONEN

Es wurde sorgfältig geprüft, welche Folgen mit den einzelnen Optionen für die Sicherheit, die Wirtschaft und die Menschenrechte verbunden sind. Die Folgen für die Sicherheit kommen im Wesentlichen in Form einer Stärkung der Strafverfolgungsbehörden in rechtlicher oder operativer Hinsicht zum Tragen. Die Folgen für die Wirtschaft umfassen Kosten für die Behörden und den privaten Sektor; es ist zwischen direkten und indirekten Auswirkungen zu unterscheiden. Die Folgen für die Menschenrechte umfassen direkte Auswirkungen auf die Freiheit der Meinungsäußerung und indirekte Auswirkungen auf das Recht auf Leben und das Recht auf körperliche und geistige Unversehrtheit. Nach sorgfältiger Prüfung der Folgen, die mit jeder einzelnen Option für die Sicherheit, die Wirtschaft und die Menschenrechte verbunden sind, wurden die jeweiligen Vor- und Nachteile ermittelt.

Bei Option 1 wird das Übereinkommen des Europarats zur Verhütung des Terrorismus positive Auswirkungen auf die Sicherheit haben und dazu beitragen, den Missbrauch des Internets für terroristische Zwecke anzugehen. Diese Option impliziert eine Stärkung der Kapazitäten der Strafverfolgungsbehörden mit dem Ziel, gegen die neuen Vorgehensweisen der Terroristen, einschließlich gegen über das Internet begangene Straftaten, bei uneingeschränkter Achtung der Menschenrechte vorzugehen. Sie impliziert außerdem, dass eine weitere Regelung auf EU-Ebene nicht erforderlich ist. Eine umfassende Rechtsangleichung wird allerdings erst erreicht sein, wenn alle Mitgliedstaaten das Übereinkommen unterzeichnet und ratifiziert haben. Dieser Prozess kann sich über viele Jahre hinziehen.

Option 2 ist die extremste der geprüften Optionen. Sie bietet den Vorteil, dass die Verbreitung des betreffenden Materials über das Internet direkt an der Quelle unterbunden wird. Allerdings sind mit dieser Option schwerwiegende Nachteile verbunden. So wird das Verhalten der Personen, die terroristische Propaganda und terroristisches Wissen produzieren, nicht unter Strafe gestellt, und auch die Einhaltung der Menschenrechte ist nicht in vollem Umfang gewährleistet.

Option 3 sieht praxisbezogene Maßnahmen vor, mit denen die Strafverfolgungsbehörden in die Lage versetzt werden, die Botschaften aufzuspüren und zu analysieren, mit denen terroristische Propaganda und terroristisches Fachwissen über das Internet verbreitet werden. Diese Maßnahmen sind auch bei der Identifizierung der Autoren derartiger Botschaften hilfreich. Die auf diese Weise gesammelten Informationen ermöglichen es, terroristische

Trends zu verstehen, terroristische Straftaten zu antizipieren und Terroranschläge zu verhindern. Allerdings mangelt es an den erforderlichen Rechtsvorschriften, und so sieht diese Option weder vor, dass gegen die Verbreitung terroristischer Propaganda und terroristischen Wissens ermittelt werden darf, noch dass terroristische Aktivisten und Sympathisanten, die hinter derartigen Inhalten stecken, verfolgt werden können. Da die rechtliche Komponente fehlt, führt Option 3 nur zu einer teilweisen Stärkung der Strafverfolgungsbehörden.

Die Vor- und Nachteile von Option 4 decken sich weitgehend mit denen von Option 1.

Option 5 weist hinsichtlich der Auswirkungen auf die Menschenrechte Ähnlichkeiten mit Option 1 auf, da auch diese Option Bedingungen und Garantien des Übereinkommens des Europarats zur Verhütung des Terrorismus umfasst, die auf den Schutz der Menschenrechte und Grundfreiheiten zielen. Gleichzeitig sind mit dieser Option große Vorteile verbunden, z. B. die Anwendung der im Rahmenbeschluss enthaltenen Straf- und Zuständigkeitsvorschriften auf die in diesen Rahmenbeschluss neu eingeführten Straftatbestände. Auch würde diese Option bei den neuen Straftatbeständen die Anwendung des Europäischen Haftbefehls garantieren und die Nutzung spezieller Instrumente der EU-Kooperation ermöglichen, die mit dem Rahmenbeschluss zur Terrorismusbekämpfung verknüpft sind. Darüber hinaus weist sie alle Vorteile auf, die EU-Rechtsvorschriften gegenüber internationalen Übereinkommen und Verträgen auszeichnen.

Ausgehend von dieser Analyse erscheint eine Kombination der Optionen 3 und 5 die wirksamste Strategie zu sein, um gegen den neuen Operationsmodus der Terroristen, insbesondere den Missbrauch des Internets für öffentliche Aufforderungen zur Begehung terroristischer Straftaten sowie für die Anwerbung und Ausbildung für terroristische Zwecke vorzugehen, ohne bei den Menschenrechten Abstriche zu machen.

TEIL 7: ÜBERWACHUNG UND BEWERTUNG

Die Überwachung und Bewertung der unter Option 5 vorgesehenen rechtlichen Maßnahmen würde – in Bezug auf die Änderung des Rahmenbeschlusses des Rates zur Terrorismusbekämpfung – durch die Bewertung der auf nationaler Ebene getroffenen Durchführungsmaßnahmen nach Artikel 11 des Rahmenbeschlusses gewährleistet.

Die Überwachung und Bewertung der unter Option 3 vorgesehenen nichtlegislativen Maßnahmen würde durch die Artikel 13 und 15 des Programms „Kriminalprävention und Kriminalitätsbekämpfung“ gewährleistet. In Artikel 13 sind die Bestimmungen für die Überwachung der im Rahmen dieses Programms finanzierten Maßnahmen festgelegt; Artikel 15 enthält die Regelungen für die Bewertung des Programms insgesamt.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333